UNIVERSITÀ DEGLI STUDI DI VERONA

DIPARTIMENTO DI

SCIENZE GIURIDICHE

SCUOLA DI DOTTORATO DI

SCIENZE GIURIDICHE ED ECONOMICHE

DOTTORATO DI RICERCA IN

SCIENZE GIURIDICHE EUROPEE ED INTERNAZIONALI

CICLO /ANNO: XXXV/2019

CYBERCRIME E NUOVE FORME DI AGGRESSIONE AL PATRIMONIO. UN'INDAGINE IN PROSPETTIVA EUROPEA E COMPARATA

CYBERCRIME, EIGENTUMS- UND VERMÖGENSDELIKTE. EINE ERFORSCHUNG IN EINER EUROPÄISCHEN UND VERGLEICHENDEN PERSPEKTIVE

REALIZZATA IN COTUTELA CON L'UNIVERSITÀ DI BAYREUTH

S.S.D. IUS 17

Coordinatori: Per l'Università di Verona

Prof. Giovanni Rossi

Firma _____

Per l'Università di Bayreuth

Prof. Martin Schmidt-Kessel

Firma _____

Tutori: Per l'Università di Verona

Prof. Lorenzo Picotti

Firma _____

Per l'Università di Bayreuth

Prof.ssa Nina Nestler

Firma _____

Dottoranda: Dott.ssa Chiara Crescioli

Firma _____

Cybercrime e nuove forme di aggressione al patrimonio. Un'indagine in prospettiva europea e comparata – Chiara Crescioli
Tesi di Dottorato
Verona, 7 marzo 2023

SOMMARIO

Negli ultimi anni si è assistito ad una rapida evoluzione degli attacchi cibernetici contro il patrimonio e, più in generale, le infrastrutture critiche. I c.d. *cyber-attacchi* garantiscono ai criminali informatici ed in specie ad organizzazioni criminali la possibilità di conseguire lauti guadagni a fronte di limitate probabilità di incorrere in sanzioni penali, potendo contare sulla scarsa attenzione e sull'impreparazione delle vittime e potendo celare la loro vera identità dietro l'anonimato, che, almeno in parte, connota ancora il *cyberspace* o operando indisturbati da Paesi esteri.

Il *modus operandi* dei criminali informatici che agiscono per fini di profitto è ormai consolidato: in primo luogo si tratta di impossessarsi delle credenziali di autenticazione (*login*, *password*, ecc.) per accedere abusivamente al sistema informatico della potenziale vittima. In tal senso, vengono offesi (o messi in pericolo), non solo beni giuridici di natura patrimoniale, ma anche nuovi interessi giuridici meritevoli e bisognosi di tutela, quali la riservatezza informatica, la sicurezza informatica, l'integrità di dati e sistemi nonché l'identità digitale.

La presente tesi, che consta di sei capitoli, muove da una indagine empirico-criminologica sulle nuove forme di aggressione al patrimonio commesse mediante le nuove tecnologie (cap. I). L'obiettivo della ricerca consiste nell'individuare sul piano giuridico-penale le tecniche di tutela del patrimonio adottate dal nostro legislatore (cap. II, III e IV) e confrontarle con quelle di alcuni ordinamenti che sono oggi all'avanguardia nella protezione degli interessi patrimoniali contro le minacce provenienti dal *web*. Particolare attenzione sarà rivolta, in tal senso, agli ordinamenti penali spagnolo e tedesco (cap. V). L'indagine comparata consentirà di far emergere, da un lato, le tecniche adottate dai legislatori dei menzionati Paesi per dare attuazione agli obblighi di incriminazione europea *in subjecta materia* e, dall'altro, per far emergere gli "idealtipi" dei reati tradizionali, informatici e cibernetici posti a tutela del patrimonio. Il metodo comparato consentirà altresì di individuare i principali problemi politico-criminali e dogmatici connessi a questo peculiare settore del diritto penale ed in specie alle norme incriminatrici che puniscono anche meri atti preparatori alla commissione di più gravi reati contro il patrimonio.

In primo luogo, si provvederà a descrivere il substrato empirico-criminologico sotteso alle nuove cyber-minacce nei confronti del patrimonio, concentrando in particolare l'attenzione sulle tipologie dei comportamenti fraudolenti *online*, quali le *advance fee fraud* e gli "schemi Ponzi", sulle condotte fraudolente aventi ad oggetto i mezzi di pagamento, l'utilizzo di *ransomware* e l'impiego di criptomonete per fini di riciclaggio (cap. I). Si

verificherà, quindi, anche alla luce degli interessanti dati relativi alla c.d. cifra oscura, se le norme incriminatrici previste nel nostro ordinamento a tutela del patrimonio, siano adeguate a prevenire e contrastare i nuovi fenomeni criminosi commessi mediante l'utilizzo delle nuove tecnologie e l'IA. Particolare attenzione verrà dedicata, in tal senso, al c.d. *Cybercrime-as-a-service*, vale a dire alla messa a disposizione (sul *web* ed in specie sul *dark web*), da parte di gruppi criminali, di *skills*, risorse umane e *tools* (*malware*, *ransomware*, credenziali, ecc.) che consentono a soggetti meno esperti di conseguire illecitamente profitti online o, comunque, di commettere attività illecite.

Successivamente si confronteranno le tecniche di incriminazione adottate nel nostro ordinamento con le raccomandazioni e prescrizione di fonte europea e sovranazionale e con le tecniche legislative adottate in specie in Spagna ed in Germania.

Infine, va evidenziato che la dimensione transnazionale del *cybercrime* pone nuove sfide sia per i legislatori nazionali che per le autorità di *law enforcement*, perché la singola iniziativa presa a livello statale rischia di rivelarsi inefficace. Sarà, pertanto, approfondita l'analisi delle iniziative e fonti sovranazionali in materia, che si occupano specificamente di rafforzare la tutela del patrimonio dalle nuove minacce cibernetiche, tra cui la Convenzione *Cybercrime* del Consiglio d'Europa del 2001, che ancor'oggi costituisce il principale strumento internazionale in tale ambito a livello globale, nonché le fonti legislative adottate dall'Unione Europea. In un'ottica di diritto comparato saranno poi analizzati i testi legislativi, la giurisprudenza e gli studi dottrinali degli ordinamenti giuridici tedesco e spagnolo. In questo modo sarà possibile stabilire se le soluzioni interpretative adottate in altri Paesi con legislazione simile alla nostra possano eventualmente essere utilizzate anche per risolvere i problemi applicativi individuati nel nostro ordinamento, verificare se sia stata raggiunta l'auspicata armonizzazione penale nell'ambito del diritto penale dell'informatica ed, eventualmente, ipotizzare come il quadro giuridico europeo possa essere migliorato per garantire l'integrazione europea.

In conclusione, verranno individuate, da un punto di vista dogmatico e politico-criminale, le formulazioni normative più idonee per tutelare in modo efficace il patrimonio rispetto alle più insidiose minacce provenienti dal web. In tal senso, verranno formulate, in prospettiva de *jure condendo*, alcune concrete proposte per l'incriminazione dei nuovi fenomeni criminosi posti in essere mediante l'utilizzo indebito o illecito delle nuove tecnologie, nel rispetto dei fondamentali principi penalistici di rango costituzionale e convenzionale.

ABSTRACT

In the last decade, cyberattacks against property and critical infrastructures have spread all over the world. Hackers have new tools, such as Artificial intelligence technologies, to facilitate this kind of criminal acts and cyber vulnerabilities are exploited using simple, sophisticated or a combination of several cyberattacks. In fact, Dark web provides a marketplace for malware and stolen data, as well as services such as the distribution of spam, phishing e-mails, web hosting and proxy services which may be used for fraudulent purposes.

Multiple victims may be involved in cyberattacks, such as an individual whose identity or account details has been stolen, and the financial institution, government agency or service provider that has been duped. For this reason, cyberattacks like phishing, pharming or ransomware are a cross-cutting problem which does not only violate property, but also security and privacy of Internet users. The cost of this phenomenon extends beyond the direct financial loss, since it includes loss of consumer confidence, time loss, and the emotional impact on victims.

Cybercrimes such as computer fraud and extortion guarantee cybercriminals and criminal organizations high profits with limited chances of incurring criminal penalties, because anonymity of the Internet is a huge obstacle in order both to prevent and punish cyberattacks against property and critical infrastructure. Another problem is the trans-border character of offences committed through the Internet. Cybercrime operates outside of any geographical constraints, so cooperation between different States may not be possible if a country does not have substantive laws to prosecute or extradite the perpetrator.

The scope of this research is to analyze how new sophisticated cyberattacks can now be punished under national legislation and how substantial penal law should be modified to be effective and efficient to prosecute this kind of illegal activities without violate fundamental principles, such as the principle of legality, subsidiarity and proportionality or liability.

Chapter I focuses on the different methods used to perpetrate cyberattacks against property on the web. It describes the various forms of frauds, ranging from online advance-fee-fraud to sim swapping. It examines the techniques and hacker tools implemented by cybercriminals to lure victims online, which increasingly involve the use of phishing and malware. Furthermore, it offers an overview of the most significant European initiatives to address the issue of cybercrime, including the Council of Europe's Convention on Cybercrime and European directives.

Chapter II analyses how Italian domestic penal legislation punishes acts preparatory to illegal activities such as computer fraud or computer sabotage. It examines the problem of dual-use nature of many software and the importance of avoiding criminalization of tools produced and placed for legitimate purposes that, though they could be used to commit criminal offences, do not constitute themselves a threat.

Chapter III examines sanctions and penalties for online fraud, counterfeiting of non-cash means of payment, computer and data sabotage and other unlawful acts that consist in unlawfully obtaining monetary values from the victims.

Chapter IV focuses on the phenomenon of cyberlaundering, as new payment technologies allow their users to move funds electronically, making illegally acquired money appear as if it was derived from legitimate sources without the risks of physically moving large quantities of cash. It also analyses the role of money mules, which play a very important role in cyberlaundering and fraud networks.

Chapter V is about comparison of cybercrime domestic penal legislation in Europe. It focuses on the national cybercrime penal frameworks of Germany and Spain, in order to establish how certain cyber-attacks are punished in these countries and to determine whether full harmonization of national legislation in this area has been achieved.

Finally, chapter VI attempts to offer solutions to the different problem detected in this research and for developing an effective criminal framework adequate to punish all stages of cyberattacks against property and critical infrastructures.

INDICE

Pag.

Capitolo Secondo
L'INCRIMINAZIONE DI MERI ATTI PREPARATORI ALLA COMMISSIONE DI PIÙ GRAVI REATI *LATO SENSU* PATRIMONIALI

Capitolo Terzo
I REATI *LATU SENSU* PATRIMONIALI NELL'ORDINAMENTO ITALIANO: PROBLEMI APPLICATIVI

Introduzione

L'oggetto della presente indagine concerne la tutela penale del bene giuridico del patrimonio di fronte alle nuove forme di aggressione commesse mediante le nuove tecnologie dell'informazione e della comunicazione. I risultati della ricerca saranno esposti in sei capitoli.

Nel primo capitolo si procederà, innanzitutto, all'analisi del concetto di patrimonio in relazione all'utilizzo della rete per effettuare transazioni finanziarie di qualsiasi tipo, e delle nuove modalità di aggressione a tale bene giuridico rese possibili dall'utilizzo del *web*. Si evidenzierà poi che gli attacchi informatici si articolano di regola in più fasi, delle quali l'effettivo depauperamento della vittima costituisce la fase finale. Quindi ci si soffermerà sul ruolo del soggetto passivo. Infatti, per distrarre a loro favore valori e crediti appartenenti alla vittima, i criminali informatici necessitano prima di prendere il controllo del sistema di *home banking* accessibile a quest'ultima, tramite soprattutto la captazione delle relative credenziali di autenticazione. In tal modo, non viene leso unicamente il patrimonio delle vittime, ma anche altri beni giuridici primari, quali il diritto alla riservatezza o all'identità personale.

Poiché si tratta di fenomeni criminosi diffusi a livello globale, si esamineranno le iniziative sovranazionali in materia dirette specificamente a rafforzare la tutela del patrimonio dalle nuove minacce cibernetiche. Sarà necessario soffermarsi, quindi, sulla Convenzione *Cybercrime* del Consiglio d'Europa del 2001, che ancor'oggi costituisce il principale strumento internazionale in tale ambito a livello globale, nonché le iniziative legislative adottate dall'Unione Europea. In particolare, ci si riferisce alla direttiva 2013/40/UE relativa agli attacchi contro i sistemi di informazione, al Regolamento 2019/881/UE relativo all'ENISA, ovvero l'Agenzia dell'Unione europea per la cybersicurezza, la nuova direttiva 2022/2555/UE relativa alle misure per un livello comune elevato di cybersicurezza nell'Unione, nonché alla direttiva 2019/713/UE relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti.

Il secondo capitolo sarà dedicato ai reati prodromici alla commissione di reati contro il patrimonio in senso stretto. Infatti, le recenti scelte politico-criminali adottate in materia di criminalità informatica, sia dal legislatore europeo che da quello italiano, sono orientate alla repressione anche degli atti preparatori diretti alla commissione di più gravi reati informatici e patrimoniali, in specie frode informatica e danneggiamento informatico. Tuttavia, sebbene talune condotte, come ad esempio la messa a disposizione, diffusione o cessione delle *password* altrui illecitamente captate, siano già di per sé lesive di beni giuridici

protetti, si dovrà esaminare se con queste tecniche di tutela, che vanno ad anticipare notevolmente la soglia di rilevanza penale, non si arrivi a veri e propri reati di sospetto. Si dovrà, dunque, individuare un confine tra le condotte oggettivamente prodromiche e preparatorie, che costituiscono un pericolo per un bene giuridico di rilevante importanza e possono essere legittimamente punite, e le condotte c.d. neutre, sorrette da un mero scopo soggettivo illecito, la cui incriminazione finisce per violare le garanzie costituzionali.

Il terzo capitolo sarà dedicato alla legislazione penale italiana in materia di reati informatici contro il patrimonio e alle fattispecie tradizionali a protezione del bene giuridico del patrimonio, cui possono essere ricondotti alcuni dei nuovi fenomeni criminosi. In particolare, si esaminerà se le fattispecie di truffa ed estorsione, in mancanza di fattispecie *ad hoc* che sanzionino espressamente i nuovi fenomeni criminosi, quali ad esempio *nigerian scams* e *ransomware*, siano effettivamente adeguate a reprimerli. Si verificherà poi quali nuove forme di aggressione possano essere ricondotte alle fattispecie di frode informatica o alle diverse norme che sanzionano i danneggiamenti informatici. Infine, si esamineranno quelle fattispecie poste a tutela dei mezzi di pagamento che, sebbene non classificate tra i reati contro il patrimonio, svolgono tuttavia un ruolo cruciale nella sua protezione. In ultimo, sulla base delle risultanze che emergeranno dall'analisi, si offriranno spunti per dirimere le questioni relative ai rapporti tra le fattispecie esaminate.

Nel quarto capitolo si tratterà del fenomeno del reimpiego dei capitali illecitamente ottenuti tramite *cyberattacks*. Infatti, alla commissione di delitti contro il patrimonio sul *web* si accompagna spesso l'ulteriore attività criminosa correlata al reimpiego del denaro illecitamente ottenuto, che a volte è addirittura utilizzato per il finanziamento di gruppi terroristici. In tale capitolo si cercherà di valutare quali potrebbero essere le soluzioni più adeguate, dissuasive e proporzionate per punire tali fenomeni illeciti. Fondamentale sarà l'analisi dell'impatto della Direttiva UE 2018/843 del 30 maggio 2018, relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo, nonché della Direttiva 2018/1673/UE sulla lotta al riciclaggio mediante il diritto penale. Inoltre, nell'ambito del reimpiego di capitali illeciti a seguito di *phishing attacks* assume sempre più rilevanza il ruolo dei *financial manager*, ovvero di chi, spesso reclutato via *web*, senza essere concorso nel reato presupposto, nella consapevolezza della provenienza illecita o, comunque, accettandone il rischio, percepisca o riceva e successivamente trasferisca le somme di denaro provenienti da delitti non colposi, a seguito della prospettazione di facili guadagni in relazione alla semplicità dell'attività richiesta. Dunque, si andranno a valutare i presupposti sulla cui base il concorso di tali soggetti sia

punibile e si tenterà di risolvere il problema della notevole difficoltà nell'accertamento del dolo, tenendo saldo il principio costituzionale di colpevolezza.

Il quinto capitolo sarà dedicato all'analisi comparata. In particolare, ci si soffermerà dapprima sull'interessante legislazione tedesca in materia di *cybercrime*, che rappresenta un modello di riferimento per molti ordinamenti europei, quindi sulla legislazione spagnola. Si procederà dunque all'analisi delle più recenti riforme legislative riguardanti la criminalità informatica in Germania per attuare le citate direttive europee, in particolare la l. 61 del 10 marzo 2021 *zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln*, che ha modificato numerose fattispecie già esistenti, nonché introdotto nuove ipotesi di reato, e la l. 9 marzo 2021 *zur Verbesserung der strafrechtlichen Bekämpfung der Geldwäsche*, che ha profondamente innovato le fattispecie incriminatrici in materia di riciclaggio.

Per quanto riguarda, invece, l'ordinamento spagnolo, si analizzeranno in particolare la *Ley orgánica* 5/2010 del 22 giugno 2010, che costituisce la prima riforma legislativa sistematica che ha riguardato anche la criminalità informatica, nonché la recentissima *Ley Orgánica* 14/2022, del 22 dicembre 2022, di attuazione della direttiva 2019/713/UE, la quale ha modificato in modo significativo le fattispecie di frode informatica, falsificazione ed indebito utilizzo degli strumenti di pagamento diversi dai contanti. Verrà poi approfondita la casistica giurisprudenziale tedesca e spagnola in merito ai delitti contro il patrimonio commessi in *Internet* e verranno esaminate le soluzioni interpretative date ai punti problematici individuati. In un'ottica di diritto comparato saranno, quindi, analizzati i testi legislativi, la giurisprudenza e gli studi dottrinali dell'ordinamento giuridico tedesco e spagnolo.

Nel sesto ed ultimo capitolo si valuterà, alla stregua del principio di sussidiarietà, la legittimità delle scelte politico-criminali di ricorrere allo strumento penale per punire gli esaminati fenomeni criminosi lesivi del patrimonio altrui, con particolare riferimento alla punizione di atti preparatori. Dopodiché si verificherà se le fattispecie già esistenti nel nostro codice penale siano o meno adeguate, e le pene proporzionate e dissuasive, e se la classificazione sistematica odierna sia valida o se, invece, sia opportuno un suo ripensamento. Si esamineranno poi gli spinosi problemi dell'individuazione del *locus* e del *tempus commissi delicti* nei reati cibernetici e, attraverso la comparazione con i diversi a ordinamenti nazionali, si proverà a proporre una possibile soluzione interpretativa, per cercare di individuare un criterio univoco che renda più agevole la persecuzione di questi reati. Particolare attenzione sarà poi rivolta al problema dell'anonimato in *Internet*, come

condizione giuridica frequente, e si cercherà di trovare soluzioni al problema dell'individuazione degli indirizzi *IP* dai quali provengono gli attacchi informatici. Soprattutto si dovrà esaminare l'opportunità o meno di rendere tracciabili tutte le transazioni elettroniche ed obbligare chiunque all'utilizzo della propria identità reale in *Internet*. A tal proposito, si valuterà se la cooperazione pubblico-privato possa costituire la strategia vincente per reprimere queste manifestazioni criminose. Infine, grazie all'analisi comparata, si formuleranno alcune proposte per assicurare un efficace coordinamento tra le diverse fattispecie esistenti nel codice penale italiano, alle quali possono essere ricondotti i *cyberattacks* diretti a ledere il patrimonio altrui.

Oggetto e scopi

L'oggetto della presente indagine concerne la tutela penale del bene giuridico del patrimonio di fronte alle nuove forme di aggressione, che si basano sull'utilizzo delle nuove tecnologie dell'informazione e della comunicazione. L'analisi, dunque, è volta a definire preliminarmente il concetto penalistico di patrimonio, per soffermarsi poi sull'adeguatezza dei criteri di classificazione sistematica dei reati contro il patrimonio, da più parti ritenuto insoddisfacente. Lo scopo principale è quello di esaminare, anche in prospettiva *de jure condendo*, come garantire un'efficace tutela penale del patrimonio di fronte alle più gravi forme di criminalità che l'offendono poste in essere mediante mezzi informatici e come la stessa possa accordarsi con gli altri diritti costituzionalmente protetti, quali ad esempio il diritto alla riservatezza, il diritto all'accesso ai dati, alle informazioni e alla difesa, nonché il diritto alla libertà economica e dei commerci. Innanzitutto, si intende dimostrare come il ricorso alla sanzione penale sia tutt'ora necessario, poiché gli attacchi cibernetici diretti al patrimonio altrui ledono anche beni giuridici primari della persona, quali la riservatezza e il diritto all'identità personale. Inoltre, le modalità delle condotte che caratterizzano questi fatti di reato sono peculiari e molto insidiose e le vittime devono considerarsi particolarmente vulnerabili, impiegando molto tempo ad accorgersi che i loro dati personali, le loro credenziali, numeri di carte di credito ecc. sono nelle mani dei criminali informatici e non hanno modo di intervenire per evitare di subire una perdita economica o altre conseguenze negative, anche in tempi successivi. Pertanto, attraverso l'analisi delle fonti sovranazionali e la comparazione delle legislazioni di diversi ordinamenti, si tenterà di individuare un'efficace soluzione per reprimere gli attacchi informatici contro il patrimonio, nonché il fenomeno criminoso del *cyberlaundering*, che trova la sua fonte proprio in questi ultimi. Tramite l'analisi dei risultati raggiunti e la comparazione dei diversi modelli adottati nei vari

Stati, si valuterà quale sia stato l'impatto delle iniziative sovranazionali, se le stesse abbiano raggiunto l'obiettivo di armonizzare le legislazioni dei diversi Paesi e, infine, se le soluzioni ivi proposte siano realmente idonee a reprimere i nuovi fenomeni criminosi. Dopodiché si proverà a rispondere all'interrogativo di come possa coniugarsi la rapida evoluzione delle modalità di aggressione mediante mezzi informatici o telematici, con il principio di legalità e tassatività in materia penale. Inoltre, le nuove forme di aggressione, pur potendo in alcuni casi essere pacificamente ricondotte ai delitti tradizionali contro il patrimonio, sollevano problemi interpretativi del tutto nuovi, in specie in relazione all'individuazione del momento di consumazione del reato e del *locus commissi delicti*, dato che il *web* è un non-luogo in senso fisico, al frazionamento della condotta da parte di membri di organizzazioni criminali, che di regola operano con un riparto di ruoli, e, di conseguenza, alla possibilità di accertare i presupposti di un concorso di persone. Ulteriore scopo di questa indagine, dunque, è provare ad offrire soluzioni per risolvere tali problemi. Inoltre, si esaminerà l'opportunità o meno di rendere tracciabili tutte le transazioni elettroniche ed obbligare chiunque all'utilizzo della propria identità reale su *Internet*, tenendo conto dell'esistenza del diritto all'anonimato e del fatto che ad oggi nel mondo reale non è necessario comunicare in qualsiasi circostanza la propria identità. Infine, si cercherà di dimostrare che la cooperazione pubblico-privato può rappresentare un'efficace soluzione per consentire di prevenire e reprimere tali fenomeni criminosi, in quanto le transazioni che avvengono in *Internet* sono tutte tracciate e gli istituti di credito dispongono tutti di un sistema antifrode che consente di individuare gli indirizzi IP da cui sono partiti gli attacchi informatici. Pertanto, tali soggetti possono senz'altro fornire un significativo aiuto all'Autorità pubblica, che invece non dispone di sistemi altrettanto efficienti.

Aspetti metodologici della ricerca

Dal punto di vista metodologico si procederà innanzitutto ad analizzare il concetto di patrimonio, modo da poter verificare se ed eventualmente come lo stesso si sia evoluto a causa dell'espansione del *web* e del suo generalizzato utilizzo a livello globale per svolgere transazioni finanziarie. Si esaminerà poi il tasso d'incidenza dei reati contro il patrimonio commessi attraverso la rete e si analizzeranno le nuove modalità di commissione dei delitti contro il patrimonio *online*. Lo studio della fenomenologia, dunque delle nuove tecniche con i quali i criminali riescono a distrarre a loro favore valori e crediti appartenenti ad altri soggetti, è indispensabile per individuare quali fattispecie vigenti nel nostro ordinamento possono essere applicabili. Si procederà dapprima ad analizzare il quadro giuridico presente

a livello sovranazionale diretto ad armonizzare la risposta penale contro la criminalità cibernetica e, in seguito, il quadro normativo nazionale. L'esame di quest'ultimo partirà dalle fattispecie che incriminano i meri atti preparatori alla commissione di più gravi reati cibernetici contro il patrimonio. Dopodiché, si procederà con l'analisi delle fattispecie incriminatrici vigenti che tutelano il patrimonio *lato sensu*. Va evidenziato che lo studio riguarda non solo le fattispecie dirette a contrastare le forme "classiche" di manifestazione della criminalità informatica, quali ad esempio la frode informatica, l'accesso abusivo al sistema informatico o i danneggiamenti informatici, ma anche norme incriminatrici "comuni" poste a tutela del patrimonio *lato sensu*, in modo da verificare se queste ultime possano, in via interpretativa, essere applicabili anche a comportamenti e fatti posti in essere nel *web*. Infine, si analizzeranno specificamente le fattispecie che sanzionano il fenomeno del reimpiego di capitali illecitamente ottenuti.

Una volta completato l'esame delle fattispecie presenti nel nostro ordinamento, si procederà all'analisi comparata, in specie con riferimento alla legislazione tedesca e spagnola. Anche in questo caso saranno analizzate le singole fattispecie che tutelano il patrimonio *lato sensu*, in modo tale da verificare quali tecniche di aggressione al patrimonio che sfruttano le nuove tecnologie sono sussumibili nelle norme incriminatrici in vigore. A tal proposito, non si procederà esaminando il singolo ordinamento, ma si effettuerà un'unica analisi con riferimento alle fasi ed alle modalità dei diversi attacchi informatici contro il patrimonio, in modo tale da far emergere gli "idealtipi" dei reati tradizionali, informatici e cibernetici posti a tutela del patrimonio.

Infine, una volta terminata l'analisi comparata, si procederà, in prospettiva *de jure condendo*, ad ipotizzare soluzioni per la soluzione dei principali problemi politico-criminali e dogmatici connessi a questo peculiare settore del diritto penale.

Capitolo I

Le nuove minacce *online* al patrimonio: analisi del substrato empirico-criminologico

Sommario: 1. Il patrimonio quale bene giuridico meritevole e bisognoso di tutela penale; - 1.1. La classificazione dei reati contro il patrimonio. – 2. Oltre il patrimonio: gli interessi giuridici offesi dai nuovi fenomeni criminosi *online*; - 2.1. La riservatezza informatica; - 2.2. L'integrità e la sicurezza informatica e la tutela dei dati personali; - 2.3. L'identità digitale; - 2.4. Gli interessi sopraindividuali. - 3. L'evoluzione dei mezzi di pagamento; - 3.1. La carta moneta; - 3.2. Le carte di credito; - 3.3. Il bonifico bancario e i nuovi servizi di trasferimento di denaro; - 3.4. La moneta elettronica; - 3.5. Le criptovalute; - 3.6. I *token*. - 4. Le minacce cibernetiche al patrimonio e l'utilizzo illecito dell'intelligenza artificiale per fini patrimoniali: tasso di incidenza, dimensioni dei nuovi fenomeni criminosi e *modus operandi* dei *cybercriminali*; - 4.1. Le cyber-organizzazioni criminali; - 4.2. Il *Cybercrime-as-a-service*; - 4.3. *Dark web*, *Marketplace* e Intelligenza artificiale; - 4.4. Le criptovalute come strumento o oggetto del reato. - 5. I diversi schemi di truffe *online*: *nigerian scams*, *charity* e *dating scams*; - 5.1. I c.d. schemi Ponzi; - 5.2. Le *advance fee fraud*. - 6. *Phishing*, *Vishing*, *Pharming*, *Sim Fraud Swapping*, *Carding*, *Identity Theft*: l'evoluzione delle tecniche di *social engineering* finalizzate al fraudolento conseguimento di un ingiusto profitto; - 6.1. Il *phishing* e le sue varianti; - 6.2. Lo *sim swapping*, il *carding* e il furto d'identità digitale; - 7. Estorsioni, impiego di *ransomware* e danneggiamenti informatici; - 7.1. *Cyber extortion* e *sextortion*; - 7.2. I *ransomware*; - 7.3. I danneggiamenti informatici. – 8. Il ruolo del soggetto passivo e la c.d. cifra oscura. - 9. Le iniziative sovranazionali e gli obblighi di incriminazione europei in materia di *cybersecurity* e tutela dei mezzi di pagamento; - 9.1. La Convenzione *cybercrime*; - 9.2. La normativa dell'Unione europea. – 10. Prime conclusioni.

1. Il patrimonio quale bene giuridico meritevole e bisognoso di tutela penale.

Il bene giuridico del patrimonio trova specifica tutela nel titolo XII, «*dei delitti contro il patrimonio*», del libro secondo del nostro codice penale. Tale rubrica, che sostituisce quella «*dei delitti contro la proprietà*» prevista dal codice Zanardelli, nelle intenzioni del legislatore del 1930 avrebbe dovuto garantire maggior correttezza e precisione

terminologica[1]. Va detto, però, che il Codice Rocco non ha fornito alcuna definizione normativa di patrimonio. Ogni indagine in merito alle tecniche di tutela di tutela del patrimonio non può, pertanto, che partire una definizione di tale concetto normativo.

Preliminarmente, va evidenziato che dai delitti contro il patrimonio inteso come entità singola e individuale, sono tradizionalmente distinti, sia dalla dottrina che dal legislatore, i delitti contro l'economia[2]. Quest'ultimo concetto assume un'accezione pubblicistica e collettiva, nella quale l'attività economica è considerata come categoria di interesse generale[3]. Vanno altresì distinti dai delitti contro il patrimonio i reati fallimentari. In questi ultimi, infatti, il patrimonio del fallito non è tutelato di per sé, ma in quanto strumentale alla garanzia di altri beni quali l'amministrazione della giustizia o l'ordine economico complessivo[4]. Lo stesso dicesi per i reati societari, che ricomprendono i comportamenti illeciti che vengono in rilievo nell'esercizio di un'attività imprenditoriale svolta in forma collettiva, vale a dire da società. Anche in questo caso, in specie a seguito della riforma apportata con la l. 27 maggio 2015, n. 69, l'interesse meritevole di protezione penale viene individuato nella correttezza e trasparenza dell'informazione societaria, anche se strumentale alla tutela del patrimonio dei soci e dei creditori[5].

Le ultime tre categorie di reati, non tutelando il patrimonio in senso stretto, non saranno pertanto prese in considerazione ai fini del presente elaborato, in quanto si focalizza, come si è evidenziato, sulle offese al patrimonio in senso stretto.

---

[1] *Relazione ministeriale sul Progetto del Codice Penale*, vol. V, parte II, p. 435, par. 734.

[2] Cft. PEDRAZZI C., *La riforma dei reati contro il patrimonio e contro l'economia*, in AA. VV., *Verso un nuovo Codice Penale. Itinerari-Problemi-Prospettive*, Milano, 1993, p. 350 ss., p. 350 s.; MANTOVANI F., *Contributo allo studio della condotta nei delitti contro il patrimonio*, Milano, 1962, p. 17; MILITELLO V., voce *Patrimonio (delitti contro il)*, in *Dig. disc. pen*., vol. IX, Torino, 1995, p. 278 ss., p. 279; CARMONA A., *Tutela penale del patrimonio individuale e collettivo*, Bologna, 1996, p. 243 s.

[3] Sul concetto di economia pubblica v. per tutti FORNASARI G., *Il concetto di economia pubblica nel diritto penale. Spunti esegetici e prospettive di riforma*, Milano, 1994, *passim*, cui si rinvia per ampi riferimenti bibliografici.

[4] Cft. PAGLIARO A., *Il delitto di bancarotta*, Palermo, 1957, p. 17 ss.; PEDRAZZI C., SGUBBI F., *Reati commessi dal fallito. Reati commessi da persone diverse dal fallito*, in F. Galgano (a cura di), *Commentario Scialoja-Branca. Legge fallimentare*, Bologna, 1995, p. 5; più di recente MUSCO E., ARDITO F., *Diritto penale fallimentare*, Bologna, 2018, p. 11 ss.; NUVOLONE P., *voce Fallimento (reati)*, in *Enc. dir*., vol. XVI, Milano, 1967, p. 476 ss., p. 478.

[5] SEMINARA S., *La riforma dei reati di false comunicazioni sociali*, in *Dir. pen. proc.*, 2015, n. 7, p. 813 ss., p. 822. La precedente riforma dei reati societari di cui alla l. 3 ottobre 2001, n. 366, invece, si caratterizzava per una maggior tutela individualistica delle posizioni patrimoniali dei soci e dei creditori sociali, così FOFFANI L., *Verso un nuovo diritto penale societario: i punti critici della legge delega*, in *Cass. pen*., 2001, n. 11, p. 3246 ss., p. 3247.

I delitti contro il patrimonio concernono un ambito di criminalità che da sempre connota la società odierna, poiché sono statisticamente i più numerosi tra quelli commessi e di più frequente applicazione nelle aule giudiziarie[6].

Dato il richiamo a numerosi concetti ed istituti propri del diritto privato (proprietà, possesso, detenzione, cosa, danno, altruità, ecc.), la disciplina dei reati patrimoniali rinvia spesso al diritto civile. Per questo motivo, in dottrina si è a lungo discusso se i concetti, ai fini penali, dovessero essere ricostruiti in base al peculiare significato tecnico ad essi riconosciuto nel diritto civile. Sul punto si sono contrapposte diverse tesi.

La prima tesi, c.d. pancivilistica, che muove dalla teoria della natura meramente accessoria del diritto penale, ritiene si debba fare esclusivo riferimento alle nozioni del diritto privato[7]. Tale impostazione non pare, tuttavia, persuasiva, dal momento che porta a risultati pratici contraddittori, dato che le nozioni civilistiche, oltre ad essere state elaborate per perseguire diverse finalità, non sono sufficienti a soddisfare pienamente le peculiari esigenze di tutela del diritto penale[8]. Si aggiunga poi che neppure il diritto civile fornisce una nozione espressa di patrimonio, né lo disciplina come categoria generale[9].

Secondo la diversa tesi c.d. autonomistica, il significato da attribuirsi ai termini di origine privatistica presenti nella legislazione penale dovrebbe sempre essere determinato in modo autonomo[10]. Anche questa impostazione non è andata esente da critiche. Respingendo in qualsiasi caso ogni possibilità di corrispondenza tra nozioni penalistiche e civilistiche, questa seconda tesi pecca, rispetto alla precedente, per eccesso e si pone in contrasto coi tradizionali canoni dell'interpretazione[11].

---

[6] Cft. ISTAT, *Delitti, imputati e vittime di reati. La criminalità in Italia, attraverso una lettura integrata delle fonti sulla giustizia. Riedizione con dati aggiornati*, 2020, p. 20, disponibile al sito https://www.istat.it/it/archivio/reati.

[7] Tra i sostenitori di tale teoria v., ad es., ROCCO A., *L'oggetto del reato e della tutela giuridica penale. Contributo alle teorie generali del reato e della pena*, Torino, 1913, rist. Roma, 1932, p. 53 nota n. 52, il quale evidenzia come «*proprietà e possesso giuridicamente sono quel che sono: diritti subiettivi privati patrimoniali e più precisamente diritti reali che trovano la loro fonte nelle norme del diritto privato. Soltanto il diritto privato, non il diritto penale, può dunque dirci che cosa essi sono*»; ANGELOTTI D., *Delitti contro il patrimonio*, in E. Florian (a cura di), *Trattato di diritto penale*, IV ed. agg., Milano, 1936, p. 35 ss.

[8] NUVOLONE P., *Il possesso nel diritto penale*, Milano, 1942, p. 43 ss.; ed in specie MANTOVANI F., *Contributo allo studio della condotta nei delitti contro il patrimonio*, cit., p. 23 ss.

[9] Sul concetto di patrimonio nel diritto civile v. TRABUCCHI A., *Istituzioni di Diritto Civile*, L ed. a cura di G. Trabucchi, Milano, 2022, p. 763; BIANCA M., *Diritto civile*, vol. VI, La proprietà, Milano, 2017, p. 35 e 103 ss.; GAMBARO A., *La proprietà. Beni, proprietà, possesso*, Milano, 2017, p. 1 ss.

[10] Così PETROCELLI B., *L'appropriazione indebita*, Napoli, 1933, p. 86, secondo cui: «*Il diritto civile deve senza dubbio restare quello che è, ma anche il diritto penale deve restare quello che è, e nessuno potrà pretendere che il contenuto di qualcuna delle sue norme debba essere diverso da quello che, in effetti, il legislatore ha voluto, sol perché si è avvalso di un termine che nel diritto privato è assunto con una significazione diversa*».

[11] ANGELOTTI D., *op. cit.*, p. 19 ss.

Maggior consenso pare trovare oggi in dottrina la tesi c.d. scettica, secondo la quale i concetti penalistici non necessariamente coincidono con quelli del diritto civile, ma neppure sono totalmente autonomi rispetto ad essi[12].

Per quanto riguarda poi specificamente la definizione "penalistica" di patrimonio, tradizionalmente si distinguono tre concezioni fondamentali: giuridica, economica ed economico-giuridica[13].

Per la prima il patrimonio è il complesso dei beni economici che appartengono ad un dato soggetto. In tal senso essa verrebbe a tutelare soltanto le cose aventi un obiettivo valore economico, valutabile in denaro[14]. Tale ricostruzione del concetto di patrimonio non è andata esente da critiche, dal momento che non solo lascerebbe prive di tutela le cose aventi un mero valore affettivo, ma non consentirebbe neppure di sanzionare le aggressioni che diminuiscono la loro capacità strumentale di soddisfare i bisogni del soggetto, oltre a non essere idonea a spiegare l'incriminazione di fatti concretantisi in una mera turbativa dell'altrui pacifico godimento del bene[15].

Per la contrapposta concezione giuridica, il patrimonio sarebbe il complesso dei rapporti giuridici, economicamente valutabili, che fanno capo ad una persona[16]. Anche tale tesi ha sollevato perplessità. Secondo alcuni studiosi essa peccherebbe per eccesso, in quanto porterebbe ad incriminare la mera alterazione del rapporto giuridico con la cosa, anche qualora non portasse ad alcuna diminuzione dell'entità della *res* ad essa connessa o utilità. La concezione giuridica anticiperebbe inoltre la realizzazione del danno e, di conseguenza, la perfezione dei reati posti in essere con la cooperazione artificiosa della vittima (ad es. truffa ed estorsione) al momento della realizzazione dell'atto dispositivo, ovvero della costituzione del rapporto giuridico svantaggioso[17]. Al fine di superare i limiti e gli eccessi di tutela delle due menzionate concezioni, è prevalsa, tanto in dottrina quanto in giurisprudenza, una terza definizione c.d. giuridico-funzionale di patrimonio, secondo la quale ai fini penali, esso sarebbe integrato dal complesso di rapporti giuridici facenti capo

---

[12] In tal senso v. PECORELLA G., voce *Patrimonio (delitti contro il)*, in *Noviss. Dig. it.*, vol. XII, Torino, 1965, p. 628 ss., p. 632 ss.

[13] Cft. MANTOVANI F., *Contributo allo studio della condotta*, cit., p. 7 ss. Nella manualistica v., per tutti, FIANDACA G., MUSCO E., *Diritto penale, Parte speciale*, vol. II tomo 2, I delitti contro il patrimonio, Bologna, 2015, p. 23 ss.

[14] BETTIOL G., *Concetto penalistico di patrimonio e momento consumativo della truffa*, in *Giur. it.*, 1947, parte IV, disp. I; DE MARSICO A., *Delitti contro il patrimonio*, Napoli, 1951, p. 11.

[15] ANGELOTTI D., *op. cit.*, p. 57 ss.

[16] Verosimilmente si tratta della concezione accolta dal nostro legislatore, v. la *Relazione ministeriale sul Progetto del Codice Penale*, cit., p. 435.

[17] MANTOVANI F., voce *Patrimonio (delitti contro il)*, in *Enc. Giur.*, Roma, 1991, vol. XXV, p. 4 ss.

ad una persona ed aventi pur sempre per oggetto cose dotate di una funzione strumentale, della capacità, cioè di soddisfare bisogni materiali o spirituali[18].

In quanto incentrata sul complesso dei rapporti giuridici, la definizione giuridico-funzionale consente di ricomprendere nel concetto di patrimonio anche le aggressioni che non comportino una diminuzione economica, pur alterandone la strumentalità, e che si concretino in una mera turbativa del godimento del bene aggredito.

Quest'ultima concezione considera essenziale per la valutazione dell'esistenza dell'offesa non tanto il saldo negativo che deriva dalla diminuzione ed accrescimento di singole sue parti, bensì la diminuzione della disponibilità economica del suo titolare, che è collegata al mutamento delle componenti patrimoniali. In questo modo sarebbe possibile raggiungere un elastico adattamento dell'offesa agli effettivi interessi economici del soggetto titolare, nonché l'ingresso di prospettive di personalizzazione, così come richiesto dalla Costituzione, da individuarsi nella valutazione del mancato raggiungimento di scopi patrimoniali[19].

Un autorevole settore dottrinale ha sostenuto l'inadeguatezza delle tre le concezioni di patrimonio sopra descritte, evidenziando che avrebbero il difetto di considerare il patrimonio non come unità strutturata secondo esigenze personali, ma come una mera somma di singole componenti[20]. In tal senso, si è evidenziato che il patrimonio costituirebbe un'unità strutturata secondo le finalità della persona, per cui la sua tutela non dovrebbe mirare ad assicurare l'integrità di un astratto valore in denaro, ma avrebbe il compito di garantire il bene, nella sua conformazione individualizzata, contro ingiustificate ed illecite diminuzioni[21].

A prescindere dall'adesione ad una delle menzionate tesi, occorre evidenziare, in questa sede, che il peculiare contenuto della categoria dei reati contro il patrimonio va ricercato nella natura patrimoniale degli interessi giuridici offesi. L'elemento costitutivo di ogni fattispecie è, in tale ambito, un'offesa (o messa in pericolo) al bene giuridico del patrimonio[22]. Il Titolo XII del libro secondo del codice penale comprende non soltanto illeciti penali offensivi di interessi patrimoniali, ma anche numerosi reati plurioffensivi (ad es. rapina, estorsione, ecc.), la cui commissione aggredisce anche altri beni giuridici, quali ad esempio l'integrità fisica o la libertà di autodeterminazione. Si aggiunga poi che la

[18] MANTOVANI F., voce *Patrimonio*, cit., p. 5; MILITELLO V., voce *Patrimonio*, cit., p. 287.
[19] MOCCIA S., *Tutela penale del patrimonio e principi costituzionali*, Milano, 1988, p. 61 ss.
[20] *Ibid*., p. 66.
[21] *Ibid*., p. 70.
[22] MANTOVANI F., *Contributo allo studio della condotta*, cit., p. 16.

categoria dei reati contro il patrimonio dev'essere individuato in modo da ricomprendere ogni illecito penale lesivo di un interesse patrimoniale[23].

Nel Titolo XII del libro secondo del codice penale sono contenuti solo alcuni dei delitti che, offendendo beni patrimoniali, possono essere ricondotti alla categoria dei reati contro il patrimonio, basti pensare all'abuso di carte di credito, situato in un diverso titolo del codice penale[24]. Per rintracciare nel nostro ordinamento i reati che tutelano il bene giuridico del patrimonio occorre, dunque, riportarsi ai fondamenti ed ai criteri della teoria generale del reato, ed in specie alla teoria del bene giuridico individuando in particolare la natura (o qualità) dell'interesse protetto, vale a dire, nello specifico, la patrimonialità di un diritto o di un rapporto, che è data unicamente dalla loro natura economica, muovendo dalle peculiari forme di aggressione[25].

Nei reati contro il patrimonio, il bene giuridico tutelato si presenta come un diritto soggettivo individuale. Si protegge, quindi, un rapporto di "signoria" di un individuo su un oggetto. Di conseguenza, il delitto contro il patrimonio si manifesta come un comportamento di aggressione o messa in pericolo di questa relazione con la *res*[26]. I delitti contro il patrimonio hanno sempre come punto di riferimento una "cosa"[27]. Ed in questo senso i giudici di legittimità hanno stabilito, in più occasioni, che nei reati contro il patrimonio l'oggetto giuridico «*è il patrimonio, e cioè le cose materiali in sé considerate*»[28]. Questo aspetto, come si avrà modo di evidenziare nel prosieguo (v. *infra*, cap. II, par. 9), non è affatto secondario ed ha rilevanti ripercussioni sul piano sistematico ed applicativo.

Il concetto tradizionale di "cosa" in senso giuridico non coincide con quello di "bene"[29]. Nell'ambito dei tradizionali reati contro il patrimonio, per "cosa" si intende, di regola, ogni entità materiale del mondo esteriore, diversa dall'uomo (e da un cadavere), avente la capacità strumentale di soddisfare un bisogno umano, materiale o spirituale e, in quanto tale, di formare oggetto di diritti patrimoniali[30]. Sono cose, ad esempio, gli oggetti corporali aventi un valore di scambio o anche soltanto affettivo ovvero rispondenti ad un interesse soggettivo a possederli. Lo stesso dicasi per le energie aventi valore economico,

---

[23] GREGORI I., *Delitti contro il patrimonio e patrimonio dello Stato*, in *Annali dir. proc. pen*., 1935, p. 1171 ss., p. 1172.
[24] MILITELLO V., voce *Patrimonio*, cit., p. 296.
[25] ANGELOTTI D., *op. cit.*, p. 7.
[26] SGUBBI F., *Uno studio sulla tutela penale del patrimonio*, Milano, 1980, p. 128
[27] MANTOVANI F., *voce Patrimonio*, cit., p. 5.
[28] Cass. pen., sentenza 25 aprile 1934, in *Riv. it. dir. pen*., 1935, p. 656 ss., p. 658, con nota di FRISOLI F.P., *Oggetto della tutela penale nei delitti contro il patrimonio*.
[29] ANGELOTTI D., *op. cit.*, p. 54.
[30] MANTOVANI F., *voce Patrimonio*, cit., p. 5.

che il codice penale, all'art. 624 co. 2 c.p., include espressamente nella definizione legale di cose mobili[31]. L'oggetto materiale dei tradizionali reati contro il patrimonio è in molti casi la cosa mobile, vale a dire quella che si può materialmente spostare dalla sfera patrimoniale altrui alla propria e, in definitiva, essere oggetto di impossessamento.

Il legislatore ha a lungo trascurato la tutela della quasi totalità dei "beni immateriali", ad eccezione dell'energia elettrica e di ogni altra energia avente valore economico (art. 624, co. 2 c.p.). Tuttavia, con lo sviluppo delle tecnologie dell'informazione e della comunicazione (di seguito TIC) si è avvertita l'esigenza di reprimere le aggressioni commesse a danno delle nuove entità immateriali aventi carattere economico (ad es. dati e programmi informatici rispetto ai danneggiamenti informatici) ovvero delle emergenti forme di circolazione della ricchezza. Si pensi, in tal senso, ai trasferimenti elettronici di fondi e, più in generale, ai molteplici ambiti di manifestazione delle frodi informatiche, la cui incidenza si è proporzionalmente accresciuta in relazione alla creazione ed alla diffusione degli strumenti informatici[32].

Alla luce dell'odierno modello economico, la tradizionale tutela penale del patrimonio pare obsoleta, non essendo in grado di adattarsi alla complessità ed alla rapidità che connota gli attuali rapporti patrimoniali e transazioni economiche. Rispetto a beni giuridici "emergenti" la tutela dei diritti di signoria sulle "cose" appare inadeguata, dato che i rapporti patrimoniali, nella realtà contemporanea, possono concernere oggetti dematerializzati o immateriali. Si pensi, ad esempio, ai *software* o ai dati informatici. Lo stesso dicasi per i diritti di credito, che acquistano autonomo contenuto laddove si accolga una concezione dinamico-funzionale del patrimonio[33], e che diventano estremamente rilevanti in relazione ai nuovi strumenti di pagamento.

L'assolutezza e l'esclusività della tradizionale concezione "materiale" (e "tangibile") del patrimonio sono state di recente messe in discussione. Il nostro legislatore, nell'apprestare una specifica tutela ai beni giuridici offesi (o messi in pericolo) dalle minacce cibernetiche, ha, infatti, tutelato (anche) sul piano penale aspetti immateriali dei beni patrimoniali. Ed in questo senso, in linea con quanto avvenuto in altri ordinamenti giuridici, ha progressivamente inserito nel codice penale nuovi delitti contro il patrimonio per contrastare forme di aggressione poste in essere mediante mezzi informatici[34]. Anche la

[31] *Ibid*.
[32] In argomento v. SOLA L., *Tutela dei beni immateriali e reati contro il patrimonio: alcune osservazioni*, in *Ind. pen*., 1990, n. 3, p. 782 ss., p. 783, ed ivi riferimenti bibliografici.
[33] MOCCIA S., *op. cit.*, p. 83 ss.
[34] MILITELLO V., *voce Patrimonio*, cit., p. 279.

giurisprudenza, in modo per vero non convincente, ha tentato in più occasioni di estendere l'ambito di applicazione di fattispecie tradizionali (ad es. il furto e l'appropriazione indebita) mediante una interpretazione estensiva (se non analogica) del concetto di "cosa" per ricomprendervi beni immateriali quali i dati e i sistemi informatici[35], con l'obiettivo di colmare le evidenti lacune normative presenti nel nostro ordinamento.

Il concetto di patrimonio è fortemente condizionato sul piano storico, e necessita di essere ricostruito in una dimensione dinamica, vale a dire in funzione dello sviluppo della personalità e dei rapporti patrimoniali che si instaurano nel contesto sociale. Il complesso dei reati contro il patrimonio, proprio perché disciplina l'ambito dei comportamenti economici individuali, ossia degli atti di autonomia individuale volti alla illecita circolazione, all'appropriazione di cose e beni con valore economico, costituisce un settore del diritto penale fra i più legati alla struttura economico-sociale e alle sue vicende evolutive[36]. Di conseguenza, non può rimanere ancorato a rigidi schemi, ma deve adeguarsi all'evoluzione dell'economia.

1.1. La classificazione dei reati contro il patrimonio

La mutata realtà economica e lo sviluppo delle TIC hanno messo in crisi anche la tradizionale classificazione dei reati contro il patrimonio, imperniata sulla contrapposizione tra "violenza" e "frode", quali mezzi tipici di realizzazione dei fatti di reato[37]. Lo stesso legislatore del 1930 aveva previsto la menzionata ripartizione intitolando i primi due capi del titolo XII del libro secondo del codice penale «*delitti contro il patrimonio mediante violenza alle cose o alle persone*» e «*delitti contro il patrimonio mediante frode*». Già oggetto di critiche in passato[38], tale distinzione è stata mutuata dalla vecchia concezione secondo cui la delinquenza patrimoniale può manifestarsi in due modi: mediante violenza o frode.

Nell'originaria impostazione del codice Rocco, violenza sulle cose si ha allorché la cosa venga danneggiata o trasformata o ne è mutata la destinazione; violenza alla persona è ogni energia materiale o morale diretta a piegare l'altrui volontà, anche se non giunga a

[35] V. *ex pluribus* Cass. pen., sez. II, 10 aprile 2020, n. 11959.
[36] SGUBBI F., *Uno studio*, cit., p. 271.
[37] PICOTTI L. *Nuove tecnologie e beni giuridici della persona* in ID (a cura di), *Tutela penale della persona e nuove tecnologie*. *Quaderni per la riforma del codice penale*, Padova, 2013, p. 29 ss., p. 38.
[38] PECORELLA G., *op. cit*., p. 631.

lederne l'attività fisica[39]. La frode, di contro, è l'attività ingannatoria diretta a trarre in errore[40].

Il codice penale ha operato una distinzione fondamentale tra offese arrecate al patrimonio mediante una condotta unilaterale del reo ed offese realizzate con l'artificiosa cooperazione della vittima. Nel primo caso il soggetto passivo si limita a subire il reato quale mero "spettatore"; nel secondo caso quest'ultimo contribuisce alla consumazione del fatto di reato determinando mediante il suo comportamento apparentemente "volontario" il verificarsi del risultato patrimoniale pregiudizievole[41]. A parità di danno patrimoniale, l'aggressione al bene giuridico tutelato assume significati diversi a seconda che sia commessa in modo fraudolento o violento, comporti un passaggio di elementi patrimoniali da patrimonio a patrimonio ovvero si esaurisca in una mera perdita[42].

La menzionata partizione è apparsa sin dall'inizio priva fondamento sistematico e di corrispondenza al substrato criminologico e di scarsa utilità, data l'impossibilità di ricondurre non poche fattispecie (ad es. l'estorsione) all'una o all'altra categoria. Molti autori hanno comunque accolto con favore la scelta, accolta dal nostro legislatore, di aver imperniare il sistema di classificazione dei reati contro il patrimonio sulla condotta[43]. In tal senso, si è evidenziato che il riferimento all'oggetto di tutela non sarebbe di per sé sufficiente a delineare con precisione i contorni delle offese penalmente rilevanti. Tuttavia, le nuove modalità di aggressione al patrimonio, poste in essere mediante mezzi informatici, rendono difficile operare una netta distinzione tra i tradizionali concetti di violenza e frode, basti pensare alla frode informatica, dove vi è sia la violenza che la frode.

I problemi di tipo sistematico-classificatorio concernenti i reati contro il patrimonio si sono acuiti nel tempo. Lo sviluppo della normativa penale di contrasto alla criminalità informatica e cibernetica, a seguito dell'emergere di nuove forme di aggressione al patrimonio, è avvenuto senza un coerente disegno sistematico, che ha portato ad un *corpus* legislativo disorganico e frammentario[44]. Lo stesso dicasi per la legislazione in materia di tutela penale dei mezzi di pagamento. Come si esaminerà nel prosieguo (v. *infra*, par. 8),

---

[39] DE MARSICO A., *Delitti contro il patrimonio*, Napoli, 1951, p. 15.
[40] PEDRAZZI C., *Inganno ed errore nei delitti contro il patrimonio*, Milano, 1955, p. 44 ss.; PECORELLA G., *op. cit*., p. 631.
[41] MANTOVANI F., *Contributo allo studio della condotta*, cit., p. 56.
[42] *Ibid*., p. 54.
[43] MANTOVANI F., *Contributo allo studio della condotta*, cit., p. 55; MILITELLO V., voce *Patrimonio*, cit., p. 287; SGUBBI F., *Uno studio*, cit., p. 140.
[44] PICOTTI L., *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in ID. (a cura di), *Il diritto penale dell'informatica nell'epoca di Internet*, Padova, 2004, p. 21 ss., p. 22; PECORELLA C., *Il diritto penale dell'informatica*, Padova, 2006, p. 3 ss.

con riguardo alle nuove modalità di aggressione al patrimonio, è difficile distinguere tra manifestazioni criminose lesive del solo bene giuridico patrimoniale e quelle che offendono una pluralità di interessi individuali (diritto alla riservatezza, diritto all'identità personale, ecc.), nonché collettivi (o diffusi), quali, ad esempio, la pubblica fede.

La classificazione dei reati contro il patrimonio è resa ancor più problematica dal fatto che, in assenza di un intervento organico e mediato da parte del nostro legislatore, i reati informatici e cibernetici, molti dei quali sono stati inseriti nel titolo XII del libro secondo del codice penale, nonché quelli relativi ai mezzi di pagamento, collocati tra i reati contro la fede pubblica di cui al titolo VII, sono stati nel tempo oggetto di diverse modifiche legislative che ne hanno mutato la struttura in modo significativo.

L'evoluzione dei rapporti economici, giuridici e sociali impone al legislatore penale di prestare attenzione ai comportamenti caratterizzati da un'effettiva dannosità sociale, che non sempre possono essere contrastati mediante il ricorso a strumenti di controllo non incidenti sulla libertà dell'individuo[45]. Il patrimonio, infatti, è un bene giuridico che, non essendo di rango primario, a differenza della vita o dell'integrità fisica, è, comunque, di sicuro rilievo costituzionale, perché funzionale allo sviluppo della personalità[46]. Esso è riconosciuto espressamente nell'art. 42 Cost., però a livello costituzionale vengono poste al diritto di proprietà limitazioni di principio in funzione di salvaguardia di interessi superindividuali, che ne fanno perdere il carattere di diritto fondamentale[47].

Oltre all'art. 42 Cost., che rappresenta il parametro di riferimento del sistema di tutela penale in esame, rilevano anche gli artt. 41, 44 e 47 Cost., rispettivamente dedicati all'iniziativa economica privata, alla piccola e media proprietà immobiliare e al risparmio, prendendo in considerazione il patrimonio nella sua dimensione dinamica e produttrice di ulteriore ricchezza. Tali disposizioni costituiscono un ancoraggio sicuro per la legittimazione dell'intervento penale in tale ambito.

Il diritto di proprietà è riconosciuto, secondo una concezione svincolata dalla funzione sociale, anche a livello sovranazionale dall'art. 17 della Dichiarazione Universale dei Diritti dell'Uomo, dall'art. 1 del Primo Protocollo annesso alla CEDU e dall'art. 17 della Carta dei diritti fondamentali dell'Unione europea. Quest'ultimo articolo, in particolare, segna una profonda distanza dell'ordinamento europeo rispetto alla nostra Costituzione. La

[45] MOCCIA S., op. cit., p. 78.
[46] *Ibid*., p. 26.
[47] Sulla fisionomia del diritto di proprietà, alla luce delle disposizioni costituzionali, v. i rilievi di RODOTÁ S., *Il terribile diritto. Studi sulla proprietà privata*, Bologna, 1981, p. 273 ss.

proprietà, nella Carta di Nizza, non integra solamente un diritto economico sociale, ma un diritto fondamentale di libertà, soggetto a limitazioni allorché si debbano garantire altri interessi altrettanto rilevanti dell'Unione europea[48].

In definitiva, il patrimonio è un bene giuridico che assume la qualità di vero e proprio "diritto soggettivo"[49]. Conseguentemente, il sistema dei reati contro il patrimonio si connota per il suo carattere eminentemente "sanzionatorio", dal momento che la sanzione penale viene impiegata in tale ambito quale esclusivo strumento di conservazione di un interesse, meritevole e bisognoso di tutela (anche) penale, che trova altrove la sua definizione. Per questo nel titolo XII del libro secondo del codice penale vengono puniti comportamenti che si sostanziano in una violazione dei diritti soggettivi patrimoniali e che creano maggior danno o pericolo per il patrimonio della persona offesa. L'entità del danno o del pericolo per il patrimonio della persona offesa costituiscono, invece, il criterio-guida per graduare l'entità della pena[50].

Nel sistema richiamato la salvaguardia della libertà economica è di primaria importanza[51]. Dato che l'applicazione della sanzione penale può impedire, in modo totale ed assoluto, l'esercizio dell'attività economica, interdicendo radicalmente l'attuazione di un progetto o di un'iniziativa economica da parte del reo, l'ordinamento giuridico deve sì difendere i diritti patrimoniali degli individui, ma senza intervenire dinnanzi a comportamenti leciti, che costituiscono una legittima manifestazione ed estrinsecazione della libertà economica[52]. A tal proposito si è evidenziata la necessità di effettuare una selezione fra le attività umane lesive di diritti soggettivi patrimoniali[53]. In tal senso si è ritenuto che dovrebbe essere il danno a costituire il fondamento della illiceità penale patrimoniale: non sussisterebbe delitto contro il patrimonio senza che esso sia stato leso (o messo in pericolo) economicamente o ne sia stato in qualche modo diminuito il valore[54].

---

[48] SALVI C., *Neoproprietarismo e teorie giuridiche della proprietà*, in *Europa dir. priv*., 2020, n. 4, p. 1169 ss., p. 1176.
[49] SGUBBI F., voce *Patrimonio (reati)*, in *Enc. dir.*, Milano, 1982, p. 331 ss., p. 337
[50] *Ibid*., p. 338 s.
[51] *Ibid.*, p. 352.
[52] SGUBBI F., *Uno studio*, cit., p. 50. Anche se, come evidenzia FOFFANI L., *Economia, sistema bancario e intervento penale*, in *Dir. pen. proc*., 2016, n. 8, p. 985 ss., p. 988: «*un contributo essenziale all'affermazione e stabilizzazione di un "minimo etico" nella vita degli affari non può che competere certamente anche allo strumento penale*».
[53] *Ibid*., p. 35.
[54] ANGELOTTI D., *op. cit.*, p. 85; SGUBBI F., *Uno studio*, cit., p. 8; MILITELLO V., voce *Patrimonio*, cit., p. 282.

Anche in questo caso, però, si dovrebbero selezionare a fini punitivi solo i fenomeni criminosi ritenuti particolarmente dannosi[55].

Il carattere frammentario della tutela del patrimonio è coerente con l'assetto costituzionale, in quanto corollario del fondamentale principio di *extrema ratio* del diritto penale[56]. A fronte dell'emergere di nuovi fenomeni criminosi connotati da disvalore sociale, il ricorso allo strumento penale è non solo legittimo, ma persino doveroso, soprattutto con riferimento al fenomeno della criminalità economica[57].

Le nuove condotte, poste in essere mediante le TIC, che ledono il bene giuridico del patrimonio, sono molto spesso caratterizzate dalla loro insidiosità, nonché da un'indubbia dannosità sociale. Se un tempo infilando la mano nella borsetta altrui era possibile impossessarsi del portafoglio della vittima, per sottrarre ora il denaro dal c.d. portafoglio virtuale di un conto corrente occorrono mezzi informatici adeguati, capacità tecniche ed organizzazione. Pur a fronte del mutare delle nuove aggressioni, è essenziale che i confini dell'illecito penale rimangano, in ossequio al principio di tassatività, accuratamente definiti, ovvero che la legge penale individui con precisione e in modo tassativo i comportamenti penalmente rilevanti, distinguendoli da quelli giuridicamente leciti[58]. Nonostante la menzionata esigenza di tassatività sia imprescindibile, dato l'obbligo per il legislatore di rispettare i principi penalistici di rango costituzionale di legalità, precisione e determinatezza-tassatività, va evidenziato che alcune criticità in merito alla tecnica di normazione che connota i reati contro il patrimonio[59] si sono ulteriormente acuite con l'introduzione del reato di frode informatica, del c.d. microsistema normativo dei danneggiamenti informatici, e, soprattutto, a seguito delle più recenti novelle legislative per il contrasto al *cybercrime*.

La categoria dei reati contro il patrimonio presenta numerosi esempi di concorso apparente di norme, ossia di casi in cui uno stesso fatto può essere ricondotto a più norme incriminatrici (v. *infra*, cap. II, par. 10 e cap. III, par. 5). Accade di frequente che uno stesso fatto rientri contemporaneamente in più norme incriminatrici tra loro diverse e non in rapporto di specialità. In questo modo si viola il principio di tassatività, poiché la tecnica legislativa di sovrapporre più norme penali, facendo sì che uno stesso fatto possa ricondursi contemporaneamente a più incriminazioni tra loro diverse, portando ad una c.d. doppia

[55] MOCCIA S., *op. cit.*, p. 89.
[56] MOCCIA S., *op. cit.*, p. 5 nota n. 12.
[57] *Ibid.*, p. 40.
[58] SGUBBI F., *Uno studio*, cit., p. 76.
[59] MOCCIA S., *Tutela penale del patrimonio*, cit., p. 43.

tipicità, se non addirittura plurima, rende incerta l'individuazione della fattispecie penale da applicarsi nel caso concreto e il *quantum* della corrispondente sanzione penale. Al giudice spetta così uno spazio di eccessiva discrezionalità, incompatibile col dettato dell'art. 25 co. 2 Cost.[60].

La problematica della c.d. doppia tipicità, che ricomprende le ipotesi in cui uno stesso fatto può rientrare in più fattispecie al di fuori dei casi di concorso apparente, è da attribuirsi ad una imprecisa formulazione delle norme incriminatrici. Così è particolarmente rilevante nell'ambito del diritto penale dell'informatica, soprattutto con riferimento alle manifestazioni criminose dirette a ledere interessi patrimoniali (v. *infra*, cap. III, par. 5).

In definitiva, il suddetto sistema normativo, come evidenziato da attenta dottrina, necessita di un ripensamento, che tenga conto delle peculiarità dei nuovi fenomeni criminosi e sia più aderente al loro substrato empirico-criminologico. Prima, però, di avanzare, in prospettiva *de jure condendo*, alcune proposte, è necessario esaminare in che modo il bene giuridico del patrimonio possa essere aggredito mediante l'impiego delle TIC e come, di conseguenza, debbano adeguarsi le tecniche di normazione volte a garantirne un'efficace protezione.

2. Oltre il patrimonio: gli altri beni giuridici offesi dai nuovi fenomeni criminosi *online*.

2.1. La riservatezza informatica

Le nuove tecnologie hanno fatto emergere nuovi beni giuridici meritevoli e bisognosi di tutela (anche) penale, quali l'integrità, la sicurezza informatica e la riservatezza informatica[61]. Questi nuovi interessi giuridici sono assunti al rango di diritti e trovano oggi protezione attraverso la creazione di nuove fattispecie di reato.

Naturale rilievo ha acquisito il bene giuridico della riservatezza informatica, che consiste nel diritto di escludere terzi non autorizzati dall'accesso e dalla fruibilità di spazi, sistemi, dati informatici, a prescindere dal loro contenuto[62]. In dottrina si è a lungo discusso se tale bene giuridico dovesse essere qualificato come una sorta di domicilio informatico, quale «*l'espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantita*

[60] SGUBBI F., *Uno studio*, cit., p. 263.
[61] PICOTTI L., *Sistematica dei reati informatici,* cit., p. 70, secondo il quale «*si può al riguardo parlare di beni giuridici "nuovi" in quanto non trovano corrispondenza in altri preesistenti*». Più di recente v. SALVADORI I., *L'accesso abusivo ad un sistema informatico. Una fattispecie paradigmatica dei nuovi beni giuridici emergenti nel diritto penale dell'informatica*, in PICOTTI L. (a cura di), *Tutela penale della persona e nuove tecnologie, Quaderni per la riforma del codice penale,* Padova, 2013, p. 125 ss.
[62] PICOTTI L., *I diritti fondamentali nell'uso ed abuso dei social network. Aspetti penali*, in *Giur. mer*., 2012, n. 12, p. 2522 ss., p. 2528; SALVADORI I., *L'accesso abusivo ad un sistema informatico*, cit., p. 153.

dall'art. 14 della Costituzione»[63]. Inizialmente si riteneva che l'ambiente informatico fosse assimilabile al domicilio, vale a dire ad uno spazio privato in cui si svolgono le attività domestiche, contenente dati riservati e da conservare al riparo da ingerenze e intrusioni altrui[64]. Si è, però, giustamente osservato che il *cyberspace* non è soggetto ai limiti spazio-temporali dei luoghi reali[65] e che nello spazio virtuale frequentemente si memorizzano o elaborano dati del tutto privi di contenuti personalistici[66]. In tale peculiare contesto, ciò che è meritevole di protezione non è soltanto il contenuto (personale, riservato o segreto) delle informazioni contenute in suddetti spazi ovvero dei messaggi e delle conversazioni trasmesse o ricevute da un sistema informatico, ma anche il libero, esclusivo e pacifico godimento dei nuovi ambiti, spazi o dispositivi informatici. La piena estrinsecazione della persona dipende invero anche dalla facoltà di poter disporre di sfere (virtuali) autonome, nell'ambito delle quali esercitare le proprie libertà e comunicare in modo sicuro senza interferenze altrui[67]. Più che di domicilio informatico, pare pertanto più corretto parlare, in linea con la più autorevole dottrina, di riservatezza informatica[68].

La riservatezza informatica è il primo ed ulteriore bene diverso dal patrimonio che può essere leso dalle aggressioni informatiche. Gli attacchi informatici contro il patrimonio quasi mai ledono soltanto gli interessi patrimoniali delle vittime, venendo ad incidere anche su altri beni giuridici di primaria importanza. Il danno economico, infatti, non è mai immediato, ma si verifica a seguito della realizzazione di diversi comportamenti. I criminali informatici entrano in possesso delle informazioni personali della vittima, necessarie per accedere ai conti correnti *online*. Per effettuare la disposizione patrimoniale in luogo del soggetto passivo, o per intercettarne una a lui non diretta, il criminale ha la necessità di

---

[63] V. la Relazione del Disegno di legge n. 2773, presentato dal Ministro di Grazia e Giustizia. – "Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica" (XI Legislatura, divenuto Legge 23 dicembre 1993, n. 547).

[64] In questo senso v. GALDIERI P., *Teoria e pratica nell'interpretazione del reato informatico*, Milano, 1997, p. 147; PICA G., *Diritto penale delle tecnologie informatiche*, Torino, 1999, p. 61 ss.; PLANTAMURA V., *Domicilio e diritto penale nella società post-industriale*, Pisa, 2017, p. 187 s. In giurisprudenza v. anche Cass. pen., sez. VI, sentenza 4 ottobre 1999, n. 3065.

[65] SALVADORI I., *I reati contro la riservatezza informatica*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (a cura di), *Cybercrime*, Torino, 2019, p. 655 ss., p. 660; PIERGALLINI C., *I delitti contro la riservatezza informatica (artt. 615-ter, 615-quater, 615-quinquies)*, in C. Piergallini, F. Viganò, M. Vizzardi, A. Verri (a cura di), *I delitti contro la persona. Libertà personale, sessuale e morale, domicilio e segreti*, in *Trattato di diritto penale. Parte speciale*, diretto da G. Marinucci e E. Dolcini, Padova, 2015, vol. X, p. 769 ss., p. 772; PICOTTI L., *La tutela penale della persona e le nuove tecnologie dell'informazione*, in ID (a cura di) *Tutela penale della persona e nuove tecnologie*, Padova, 2013, p. 29 ss., p. 33.

[66] BERGHELLA F., BLAIOTTA R., *Diritto penale dell'informatica e beni giuridici*, in *Cass. pen*., 1995, n. 9, p. 2329 ss., p. 2333; PICOTTI L., *Sistematica*, cit., p. 78.

[67] SALVADORI I., *I reati contro la riservatezza informatica*, cit., p. 660.

[68] Così PICOTTI L., *Sistematica*, cit., p. 78; PECORELLA C., *Il diritto penale dell'informatica*, cit., p. 322, che evidenzia come la riservatezza informatica consenta di superare «*le incertezze e le ambiguità che caratterizzano il concetto di "domicilio informatico*"».

introdursi nel sistema informatico. Dunque, l'intrusione non autorizzata nel *device* della vittima, l'intercettazione di dati, comunicazioni, codici, ecc. sono senz'altro comportamenti che ledono o mettono in pericolo beni giuridici diversi dal patrimonio.

2.2. L'integrità e la sicurezza informatica e la tutela dei dati personali

Altro bene strettamente correlato alla riservatezza informatica che viene in considerazione in quest'ambito è l'interesse all'integrità di dati e di sistemi informatici e, in generale, alla sicurezza informatica, che concerne la pronta e corretta utilizzabilità e disponibilità degli strumenti informatici[69]. Si distingue, però, dal primo poiché si presenta come strumentale rispetto alla riservatezza dei dati contenuti nel sistema, motivo per cui costituisce autonomo diritto[70]. Il bene giuridico sottostante, ovvero la garanzia di pronta e corretta utilizzabilità di dati e sistemi informatici rispetto al pericolo di alterazione, distruzione, dispersione e impedimento anche temporaneo della loro disponibilità o fruibilità, viene in rilievo non solo nei casi in cui il reo danneggi effettivamente il dispositivo, ma anche quando si limiti ad installare un *malware*. Questo perché tale codice maligno lede la garanzia del corretto funzionamento del sistema informatico, il quale diviene non più affidabile nel compiere operazioni quali la semplice digitazione di un codice.

Ulteriore interesse che viene ad essere leso dalle nuove manifestazioni criminose commesse mediante le nuove tecnologie quello alla protezione dei dati personali. Tale bene giuridico è assurto al rango di vero e proprio diritto, sancito a livello sovranazionale dall'art. 8 della Carta dei diritti fondamentali dell'Unione europea (c.d. Carta di Nizza) e dal Regolamento 2016/679/UE del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, nonché a livello italiano dall'art. 1 del d.lgs. 30 giugno 2003, n. 196, (c.d. Codice *privacy*). Trattasi di diritto autonomo rispetto al diritto alla riservatezza[71], dal momento che il diritto alla protezione dei dati personali riguarda, in generale, i «trattamenti» di dati, che possono essere effettuati anche senza l'ausilio di strumenti elettronici, per cui va ben oltre la "mera" dimensione informatica[72]. Non tutte le manifestazioni criminose nei confronti del bene *lato sensu* patrimoniale lesive del diritto ai dati personali sono lesive anche del diritto alla

[69] MANTOVANI M., *Brevi note a proposito della nuova legge sulla criminalità informatica*, in *Crit. dir.*, 1994, IV, p. 12 ss., p. 18 s.; PICOTTI L., *Sistematica*, cit., p. 70;
[70] PICOTTI L., *Sistematica*, cit., p. 77.
[71] MANNA A., DI FLORIO M., *Riservatezza e diritto alla* privacy*: in particolare, la responsabilità per* omissionem *dell'Internet provider*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (a cura di), *Cybercrime*, Torino, 2019, p. 891 ss., p. 892.
[72] SALVADORI I., *I reati contro la riservatezza informatica*, cit., p. 663.

riservatezza informatica. Qualora il criminale si limiti a clonare i dati di una carta di credito tramite uno *skimmer* e poi li venda o li utilizzi per effettuare disposizioni patrimoniali non autorizzate, viene in rilievo soltanto il diritto alla protezione dei dati personali, non quello alla riservatezza.

La nozione di "dato personale" è particolarmente ampia e comprende «*qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*»[73]. Anche i numeri di telefono, dei conti correnti e delle carte di credito o di pagamento, *passwords*, credenziali, ecc. possono rientrare nella nozione di "dati personali". Si tratta, infatti, di informazioni relative ad una persona fisica riconducibili all'identificazione[74]. La protezione prevista dall'ordinamento in quest'ambito non esclude qualsiasi trattamento o circolazione di dati personali altrui, ma è volta a garantire che vi siano delle regole da osservare per il loro trattamento, il quale deve conformarsi ai principi di lealtà, di conformità a determinate finalità, del consenso dell'interessato e all'importanza del controllo da parte di un'autorità indipendente[75]. Tali principi vengono senz'altro violati dai criminali informatici sia quando intercettano dati destinati a rimanere riservati sia, soprattutto, quando li divulgano anche sul *dark web* in cambio di un corrispettivo o comunque per fini illeciti.

2.3. L'identità digitale

Queste nuove manifestazioni possono incidere anche sulla c.d. identità digitale. L'identità digitale può, in tal senso, essere sia quella della stessa vittima (come nei casi di *phishing*), sia quella di soggetti estranei al reato, che in questo modo diventano vittime a loro volta (come avviene in quei casi in cui il criminale informatico utilizzi il nome di persone realmente esistenti per perpetrare truffe *online* senza essere scoperto, oppure costruisca siti fasulli utilizzando nomi, ditte, marchi realmente esistenti).

---

[73] Art. 4 del Regolamento 2016/679/UE.

[74] In tal senso v. anche Cass. pen., sez. III penale, sentenza 17 febbraio 2011, n. 21839, che ha classificato il numero di utenza cellulare come un dato personale. Nello stesso senso v. Cass. pen., sez. III penale, sentenza 14 novembre 2019, n. 46376.

[75] PICOTTI L., *La tutela penale della persona e le nuove tecnologie dell'informazione*, in ID. (a cura di), *Tutela penale della persona e nuove tecnologie*, cit., p. 67.

Il diritto all'identità personale, anche se è privo di un esplicito richiamo normativo, è stato elevato dalla Corte costituzionale al rango di diritto inviolabile di ogni individuo[76]. Con l'avvento delle nuove tecnologie sono nati e si sono sviluppati nuovi segni distintivi dell'individuo[77], per cui il concetto stesso di identità personale si è evoluto, al punto da ricomprendere anche la diversa nozione di identità digitale ovvero l'identità richiesta per poter svolgere diverse attività su *Internet*[78].

Ad oggi non è stata ancora affermata l'esistenza di un vero e proprio diritto all'identità digitale. A differenza della nozione di identità personale, non esiste alcuna definizione normativa o giurisprudenziale di "l'identità digitale". Diversamente dall'identità personale, non può esistere una precisa enunciazione perché non ne esiste un'unica tipologia. L'identità digitale è composta da due fattori: il primo consiste nell'identificazione dell'esistenza del soggetto fisico, mentre il secondo attribuisce a ciascun soggetto un insieme di codici elettronici tali che, una volta introdotti in uno o più strumenti informatici, singoli o in rete, la persona possa essere identificata ricollegando i codici alla sua identità[79].

Vi sono le identità digitali c.d. necessarie, vale a dire strettamente correlate all'identità personale del soggetto utilizzatore, perché richieste anche dalla legge per poter usufruire di determinati servizi pubblici o di interesse pubblico o per l'esercizio di determinate attività (posta elettronica certificata per poter contattare la pubblica amministrazione, libretti universitari elettronici, *account* per i servizi bancari, ecc.)[80]. Vi

---

[76] La Corte cost., sentenza 3 febbraio 1994, n. 13, infatti, ha statuito che «*è certamente vero che tra i diritti che formano il patrimonio irretrattabile della persona umana l'art. 2 della Costituzione riconosce e garantisce anche il diritto all'identità personale. Si tratta - come efficacemente è stato osservato - del diritto ad essere se stesso, inteso come rispetto dell'immagine di partecipe alla vita associata, con le acquisizioni di idee ed esperienze, con le convinzioni ideologiche, religiose, morali e sociali che differenziano, ed al tempo stesso qualificano, l'individuo*», così.

[77] LA TORRE M., *Il nome: contrassegno dell'identità personale*, in *Giust. civ*., 2013, n. 9, p. 443 ss., p. 444, il quale richiama ad es. *nick name, user name,* firma digitale, ecc.

[78] Cfr. COCUCCIO M.F., *Il diritto all'identità personale e l'identità "digitale",* in *Dir. fam. e pers.*, n. 3, 2016, p. 949 ss., p. 955.

[79] *Ibid*., p. 955.

[80] Un esempio significativo di identità digitale c.d. necessaria è la posta elettronica certificata per i professionisti. L'art. 6-*bis* d.lgs. 7 marzo 2005, n. 82 stabilisce che: «*al fine di favorire la presentazione di istanze, dichiarazioni e dati, nonché lo scambio di informazioni e documenti tra la pubblica amministrazione e le imprese e i professionisti in modalità telematica, è istituito, entro sei mesi dalla data di entrata in vigore della presente disposizione e con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente, il pubblico elenco denominato Indice nazionale degli indirizzi di posta elettronica certificata (INI-PEC) delle imprese e dei professionisti, presso il Ministero per lo sviluppo economico*» ed al secondo comma: «*Gli indirizzi PEC inseriti in tale Indice costituiscono mezzo esclusivo di comunicazione e notifica con i soggetti di cui all'articolo 2, comma 2*». In seguito, il d.l. 16 luglio 2020, n. 76, contenente "Misure urgenti per la semplificazione e l'innovazione digitale", convertito nella legge 11 settembre 2020, n. 120, ha disposto l'applicazione di sanzioni amministrative per tutte le imprese e i professionisti che non abbiano comunicato il proprio domicilio digitale (posta elettronica certificata) entro la data del 1° ottobre 2020.

sono poi identità digitali che un soggetto crea a proprio piacimento per compiere determinate azioni in rete (creare un *account* su un *social network*, un indirizzo *e-mail,* una registrazione su un sito di *e-commerce*, ecc.), nelle quali, però, non è richiesta la previa identificazione. Più che un'unica definizione vi potranno pertanto essere diverse definizioni, dedicate alle diverse tipologie di identità digitali. Tuttavia, tutte le tipologie sono meritevoli di tutela. L'identità digitale, anche se consiste in un mero insieme di attributi identificativi, è ciò che consente alla persona di interagire con altre persone nel *cyberspace* e di usufruire di servizi anche essenziali. Nelle mutate condizioni socioeconomiche della società, la libera costruzione dell'identità personale può essere messa in pericolo non soltanto da ipotesi di travisamento o de-contestualizzazione da parte dei *mass-media*, ma anche dal flusso delle informazioni, che riguardano la persona che non avviene attraverso canali trasparenti e all'interno di un ben preciso quadro di garanzie[81]. Diviene fondamentale, dunque, tutelare queste, seppur piccole, manifestazioni della personalità dell'individuo rispetto ai menzionati nuovi fenomeni criminosi.

Secondo una parte della dottrina, il codice della *privacy* non si occuperebbe soltanto della tutela del dato personale, ma anche dell'identità personale in quanto autonomo bene giuridico. I dati personali, infatti, non sarebbero altro che una sfaccettatura di quest'ultima[82]. Pertanto, il diritto all'identità digitale finirebbe sostanzialmente per coincidere col diritto alla tutela dei dati personali. Questa tesi, che si è affermata nell'ambito della teoria c.d. monista dei diritti della personalità, ritiene che in realtà non esisterebbero distinti diritti della personalità, ma un unico diritto della personalità. Ad essa si è contrapposta una seconda teoria, c.d. pluralista, secondo la quale i diritti della personalità sono diritti distinti e come tali vanno considerati, nonostante l'indubbia presenza di caratteristiche comuni[83].

A favore della teoria monista si sono pronunciati ampi settori della dottrina[84] e della giurisprudenza[85]. Tale tesi, con riferimento ai diritti della personalità nel *cyberspace*, è stata

---

[81] In tal senso RESTA G., *Identità personale e identità digitale,* in *Dir. inf. inf*., 2007, n. 3, p. 511 ss., p. 516.
[82] FINOCCHIARO G., *Identità personale su internet: il diritto alla contestualizzazione dell'informazione,* in *Dir. inf. inf.*, 2012, n.3, p. 383 ss., p. 388.
[83] CASSANO G., *Contenuto e limiti del diritto all'identità personale (in margine allo sceneggiato sul caso "Re Cecconi"),* in *Dir. inf. inf*., 1997, n.1, p. 118 ss., p. 121.
[84] Così FINOCCHIARO G., *La protezione dei dati personali e la tutela dell'identità*, in G. Finocchiaro, F. Delfini, *Diritto dell'informatica*, Torino, 2014, p. 151 ss., p. 155.
[85] In particolare la Cassazione, sul caso Veronesi, ha statuito che «*nel nostro diritto positivo non è dato qualificare i vari diritti della personalità come profili od aspetti di un unico ed onnicomprensivo diritto della personalità, essendo ciascuno di essi riconosciuto a tutela della varietà degli interessi fondamentali dell'uomo, ma, pur costituendo tali diritti distinti ed autonome situazioni giuridiche soggettive, si riconducono tutti ad valore integrale ed unitario della persona umana, così come è, questa, intesa nell'art. 2 Cost.*» (Cass. civ., sez. I, sentenza 22 giugno 1985, n. 3769).

accolta anche dalla Corte costituzionale tedesca, la quale ha affermato che il generale diritto della personalità è comprensivo del diritto fondamentale di garantire la riservatezza e l'integrità dei sistemi informatici[86]. In linea con quest'ultima tesi, l'identità digitale, essendo un aspetto dell'individualità che si manifesta in una realtà virtuale, rientrerebbe nel più generale diritto della personalità. Questa visione ha l'indubbio pregio di configurare una protezione più ampia, che non si limita ad esplicite previsioni normative, ma configura una forma di tutela più vasta e generalizzata.

Un orientamento giurisprudenziale[87] si è però pronunciato a favore di una tesi pluralista, distinguendo tra il diritto all' identità personale e quello alla riservatezza: il primo perseguirebbe un obiettivo "positivo" alla fedeltà della rappresentazione all'esterno di proprie vicende personali; il secondo, invece, uno "negativo" alla loro non raffigurazione[88]. Si deve ricordare, però, che «*tali distinzioni non devono naturalmente negare il carattere solidale di tali interessi, confluenti in un valore unitario, che è quello della persona umana*»[89]. Tale tesi appare adattarsi meglio ai nuovi diritti della personalità sul *web*, poiché, come si è avuto modo di evidenziare, ognuno di essi ha una sua peculiare connotazione. Peraltro, alcuni dei beni giuridici di nuova emersone, come l'identità digitale, hanno natura frammentaria, dato che ne esistono molteplici differenti tipologie, per cui difficilmente possono essere riconducibili ad un'unità.

A prescindere dall'adesione alla teoria monista o pluralista, è assodato che i nuovi fenomeni criminosi ledano non solo il patrimonio ma anche interessi giuridici correlati alla personalità dell'individuo.

2.4. Gli interessi sopraindividuali

I nuovi fenomeni criminosi non ledono soltanto beni giuridici delle vittime, ma possono anche incidere su interessi sopraindividuali. Infatti, come si avrà modo di

---

[86] V. BVerfG, sentenza 27 febbraio 2008 - 1 BvR 370/07, 1 BvR 595/07, secondo cui «*Das allgemeine Persönlichkeitsrecht (Art. 2 I i.V.m. Art. 1 I GG) umfasst das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*» (Il generale diritto della personalità (art. 2 co. 1 in combinato disposto con l'art. 1 co. 1 GG) comprende il diritto fondamentale alla garanzia della riservatezza e dell'integrità dei sistemi informatici).

[87] Cass. civ., sez. I, sentenza 7 febbraio 1996, n. 978.

[88] CASSANO G., *Contenuto e limiti del diritto all'identità personale*, cit., p. 121, secondo cui: *«da una parte, infatti, c'è l'esigenza che la rappresentazione ad altri della propria identità risponda a criteri di verità oggettiva senza false rappresentazioni o attribuzioni, dall'altra c'è l'esigenza che aspetti della propria persona rimangano sconosciuti. Due beni diversi, quindi, dettati per fini diversi, con questo, peraltro, di particolare: ove l'ordinamento sacrifichi il diritto alla riservatezza per particolari ragioni di interesse generale (...) è sempre fatto salvo l'interesse della persona affinché la medesima rappresentazione sia fedele e veridica*»: così.

[89] *Ibid*.

evidenziare in seguito (v. *infra*, cap. IV, par. 1), i criminali informatici predispongono in molti casi un'apposita trama per nascondere la provenienza illecita del denaro o delle criptovalute illecitamente sottratti. Ad essere lesi possono, dunque, essere anche l'ordine pubblico economico e l'amministrazione della giustizia[90]. Si aggiunga poi che la creazione di false identità virtuali e falsi *account* non aggrediscono soltanto l'identità personale delle vittime, ma anche la fiducia della collettività, la quale non può fare affidamento sulla lealtà delle identità con le quali mantengono rapporti virtuali[91]. Proprio perché l'utente non ha possibilità di interagire di persona con gli altri e, quindi di poter osservare *vis-à-vis* il proprio interlocutore, la fiducia assume una particolare rilevanza giuridica.

La tutela della pubblica fede riguarda anche i mezzi di pagamento. Il fatto che il sistema di pagamento debba essere utilizzato in modo corretto corrisponde ad un interesse pubblico fondamentale[92]. Solo il corretto utilizzo di tali strumenti di pagamento può garantire l'integrità complessiva del sistema bancario. Tale interesse viene offeso attraverso la mera manipolazione di tali sistemi o dal loro indebito utilizzo, a prescindere dall'effettivo conseguimento di un profitto per l'agente.

È, quindi, evidente come le nuove manifestazioni criminose ledano più interessi giuridici, non solo il patrimonio. La persona offesa oltre a subire una diminuzione del proprio patrimonio patisce anche una lesione della propria sfera più intima, della sua riservatezza e della sua qualificazione quale individuo libero di autodeterminarsi nel *cyberspace*. Una volta subito un attacco informatico, la vittima dovrà necessariamente cambiare *password*, credenziali, ecc. Ma non sempre è possibile farlo o comunque farlo tempestivamente. Basti pensare al caso in cui la vittima utilizzi, per la sua identificazione informatica, l'impronta digitale, l'iride o dati biometrici. Ancora più comunemente, al codice fiscale, utilizzato per l'identificazione. Il danno, dunque, in questi casi è ancora maggiore: una volta che un dato personale immutabile è caduto nelle mani dei criminali informatici nessun rimedio è possibile. Sarebbe, pertanto, auspicabile che il legislatore tenesse conto di quest'ultimo aspetto. Si aggiunga poi che la lesione della pubblica fede negli strumenti di pagamento ostacola lo sviluppo tecnologico, poiché aumenta la generale diffidenza nell'utilizzo dei

[90] ANTOLISEI F., *Manuale di diritto penale. Parte speciale*, vol. I, XVI ed. a cura di C.F. Grosso, Milano, 2016, p. 463; FIANDACA G., MUSCO E., *Diritto penale. Parte speciale. i delitti contro il patrimonio*, vol. III, Bologna, 2015, p. 247.
[91] MARRAFFINO M., *La sostituzione di persona mediante furto di identità digitale*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (a cura di), *Cybercrime*, cit., p. 311.
[92] Cass. pen., sez. II, sentenza 18 settembre 2020, n. 27432.

nuovi strumenti digitali, che nel nostro Paese è più alta rispetto al resto d'Europa[93].

3. L'evoluzione dei mezzi di pagamento.

3.1. La carta moneta.

L'uso del denaro contante si sta progressivamente circoscrivendo ai rapporti economici di minor valore, a favore di nuovi e diversi mezzi di pagamento, che consentono una maggior disponibilità e nel contempo tracciabilità. In questa direzione è andato anche il nostro legislatore, che allo scopo di combattere i fenomeni dell'evasione fiscale e del riciclaggio di denaro, ha imposto un tetto all'uso del contante[94], nonché l'obbligo per professionisti e negozianti di accettare le carte di debito e di credito come forme di pagamento per qualsiasi importo[95]. Tali obblighi sono rimasti in vigore anche oggi, nonostante sia stata recentemente proposta la loro eliminazione. Ad oggi, sono pochi i Paesi europei che vietano l'utilizzo del contante sopra una certa soglia (è il caso dell'Italia e della Spagna, ma non della Germania)[96]. Disporre oggi di un conto corrente bancario o postale è indispensabile per poter effettuare e ricevere pagamenti, che non vengono più effettuati in contanti.

Con il contratto di conto corrente bancario la banca si impegna ad offrire ed eseguire vari servizi per il cliente, al quale viene riconosciuta la disponibilità del saldo, che in ogni momento risulta dopo l'esecuzione delle varie operazioni di cassa, di incasso o di spese/addebiti vari. Tratto qualificante del contratto in esame è l'obbligo assunto dalla banca di provvedere per conto del cliente, e su suo ordine diretto o indiretto, a pagamenti e riscossioni nei confronti di terzi, in esecuzione di un mandato senza rappresentanza[97].

---

[93] Cft. l'indice europeo relativo al *Digital Market and Society* indica che «*Denmark, Finland, Sweden and the Netherlands have the most advanced digital economies in the EU followed by Luxembourg, Belgium, the UK and Ireland. Romania, Bulgaria, Greece and Italy have the lowest scores on the DESI*», disponibile al sito https://ec.europa.eu/digital-single-market/en/desi

[94] La prima soglia all'utilizzo del contante fu introdotta dall'art. 1 D.L. n. 143/1991, recante «*Provvedimenti urgenti per limitare l'uso del contante e dei titoli al portatore nelle transazioni e prevenire l'utilizzazione del sistema finanziario a scopo di riciclaggio*» convertito dalla L. n. 197/1991. La soglia, più volte modificata nel corso degli anni, è ad oggi tornata a 5.000 euro per effetto della Legge di stabilità per l'anno 2023.

[95] L'obbligo di dotarsi di un lettore POS (*Point of Sale*) è stato introdotto per la prima volta in Italia dall'art. 15 co. 4 del d.l. 179/12, ma non era accompagnato da nessuna sanzione. L'art. 19-*ter* l. n. 233/2021 ha poi introdotto una sanzione amministrativa pecuniaria in caso di mancata accettazione dei pagamenti con POS.

[96] Per questo motivo la Commissione europea, nel pacchetto sulle misure antiriciclaggio e contro il finanziamento al terrorismo, ha proposto di fissare in tutta l'Unione un tetto massimo sui pagamenti in contati a 10.000 euro (v. Comunicazione della Commissione relativa a un piano d'azione per una politica integrata dell'Unione in materia di prevenzione del riciclaggio di denaro e del finanziamento del terrorismo [C(2020) 2800 final]) Tuttavia, tale proposta non è ancora stata approvata dal parlamento europeo.

[97] MOLLE G., *I contratti bancari*, vol. XXXV, Tomo I, in AA.VV., *Trattato di diritto civile e commerciale Cicu-Messineo*, Milano, 1981, p. 472.

La somma di denaro depositata è, ai sensi dell'art. 1834 c.c., di proprietà della Banca e il correntista diventa titolare di un diritto di credito nei confronti di quest'ultima[98], cosa che, come si esaminerà in seguito (v. *infra*, cap. III), assume rilevanza anche per il diritto penale.

Alle volte la banca si impegna ad eseguire pagamenti anticipando fondi al cliente in virtù di un'apertura di credito. L'apertura di credito costituisce una fondamentale operazione attiva: ai sensi dell'art. 1842 c.c. è il contratto mediante il quale la banca si obbliga a mettere a disposizione al cliente una somma di denaro per un dato periodo o a tempo indeterminato. Caratteristica del contratto è la disponibilità della somma: la banca concede un c.d. fido al cliente, che può ottenere la somma a credito entro il limite previsto come massimo[99].

3.2. Le carte di credito.

Tra i moderni titoli di legittimazione al pagamento vi sono le carte di credito. Si tratta di strumenti di pagamento ad efficacia immediata, di cui esistono varie tipologie. Le carte di credito sono giuridicamente configurabili in termini di delegazioni di pagamento ad effetto immediato, attraverso cui il debitore ordina al proprio istituto di credito di riferimento di pagare il creditore, avvalendosi ai fini della legittimazione a disporre, di una carta magnetica dotata di microchip e di un codice numerico. Occorre distinguere tra carte di credito con conto corrente e carte di credito senza conto corrente che, a loro volta, sono distinguibili in carte di credito ricaricabili o c.d. usa e getta. Le prime operano nella logica della delegazione di pagamento, che trae la provvista dal conto del titolare della carta di credito. Le prepagate, invece, costituiscono carte di credito ad uso ordinario il cui rapporto di provvista non si innesta nel conto corrente bancario del titolare della carta, ma nel versamento di una somma, che rappresenta la possibilità di addebito sino al suo esaurimento. Le carte prepagate si distinguono in carte di credito ricaricabili, in cui l'importo limite a disposizione (cd. *plafond*) può essere reintegrato per il tempo di validità della carta stessa secondo le esigenze del titolare, ed in carte di credito usa e getta, emesse ad importo limite fisso, predefinito all'atto di acquisto e utilizzabili solo sino al suo esaurimento[100]. Grazie alla diffusione degli *smartphone* e degli *smartwatch*, oggi si può addirittura prescindere dal possesso materiale e dall'uso di una carta magnetica: in molti casi è, infatti, sufficiente abilitare lo *smartphone* ad effettuare pagamenti virtuali o utilizzare i soli codici numerici della carta visualizzabili

[98] Cass. civ., sez. III, sentenza 3 settembre 2019, n. 21963.
[99] MOLLE G., *op cit.*, p. 185.
[100] TRABUCCHI A., *op. cit*., p. 1538.

nell'apposita *App* per la gestione dei servizi bancari. Non solo, ma è possibile anche creare carte virtuali di pagamento usa e getta da utilizzare per gli acquisti *online*.

3.3. Il bonifico bancario e i nuovi servizi di trasferimento di denaro.

Sul piano delle operazioni di pagamento, il bonifico bancario è uno degli strumenti più diffusi e consiste in una delegazione di pagamento con cui il debitore ordina all'istituto di credito con cui ha un rapporto di conto corrente di trasferire la somma dovuta dal proprio conto al conto corrente del creditore, oggi possibili con valuta *in die*.

Gli strumenti di pagamento non sono tutti controllati da una banca centrale o da un ente pubblico. Molto diffuse sono le piattaforme di *mobile payment* (quali ad esempio *Satispay* o *PayPal*[101]) che consentono di inviare e ricevere fondi da altri utenti, utilizzatori della stessa *App*, senza utilizzare i circuiti delle carte di credito e debito tradizionali. Si tratta di sistemi che consentono di effettuare transazioni *online* senza dover necessariamente condividere i propri dati bancari e che, a differenza dei conti correnti tradizionali, non prevedono il pagamento di un canone mensile, ma solo di determinate commissioni. Tali servizi si appoggiano, comunque, alle infrastrutture finanziarie esistenti dei conti bancari e delle carte di credito[102]. Non si tratta, quindi, di mezzi di pagamento c.d. antagonisti rispetto ai mezzi di pagamento tradizionali.

Vanno richiamati, ai fini della presente ricerca, anche i sistemi telematici di trasmissione fondi internazionali (quali, ad esempio, *MoneyGram* o *Western Union*). Per eseguire una transazione è sufficiente recarsi in uno dei punti abilitati, presenti sul territorio, muniti di documento di identità e della somma da pagare, dopodiché dev'essere compilato un modulo nel quale vanno inseriti i dati richiesti, compresi quelli del beneficiario. A transizione avvenuta, viene rilasciata una ricevuta contenente il codice identificativo della transizione che, comunicato al beneficiario, gli permette di riscuotere pari somma quasi in tempo reale presso uno sportello del Paese in cui si trova. La commissione viene pagata in base alla somma inviata. Tali transazioni possono essere effettuate anche via *web* o tramite *App*[103].

---

[101] Definito come «*a secure online system that enables account holders to pay for goods or services and arrange money transfers over the Internet*». Sul punto v. voce *PayPal* in LAW J. (eds.), *A Dictionary of Accounting*, V ed., Oxford, 2016.

[102] MARTÍNEZ PEÁLEZ R., RICO NOVELLA F., *Application of Electronic Currency on the Online Payment System like PayPal*, in AA. VV. (eds.), *Project E-Society: Building Bricks*, Boston, 2006, Vol. 226, p. 44 ss., p. 47; DOMBRET B., *Zahlungssysteme im Internet. Marksituation und Perspektiven*, Norderstedt, 2008, p. 32 ss. V. quanto riportato al sito https://www.paypal.com/it/webapps/mpp/about

[103] V. https://www.westernunion.com/it/it/home.html

3.4. La moneta elettronica.

Il commercio elettronico virtuale si accompagna alla nascita e alla diffusione della *e-money*, la moneta elettronica circolante in forma digitale, che sostituisce il denaro contante e permette di effettuare acquisti di merce *online*, garantendone al tempo stesso il trasferimento. L'art. 1, co. 2, lett. h-*ter*) del decreto legislativo 1 settembre 1993, n. 385 (c.d. Testo Unico Bancario) definisce la moneta elettronica come «*il valore monetario memorizzato elettronicamente, ivi inclusa la memorizzazione magnetica, rappresentato da un credito nei confronti dell'emittente che sia emesso per effettuare operazioni di pagamento come definite all'art. 1, comma 1, lettera c), del decreto legislativo 27 gennaio 2010, n. 11, e che sia accettato da persone fisiche e giuridiche diverse dall'emittente*». La definizione riprende, quasi integralmente, quella fornita dall'art. 2, n. 2, della direttiva 2009/110/CE concernente l'avvio, l'esercizio e la vigilanza prudenziale dell'attività degli istituti di moneta elettronica[104]. In quella fornita dal legislatore europeo è ulteriormente specificato che il credito dev'essere emesso dietro ricevimento di fondi. Tale requisito non è riportato nella definizione fornita dal legislatore italiano.

Al successivo art. 114-*bis* del Testo Unico Bancario si precisa che l'emissione di moneta elettronica è riservata alle banche ed agli istituti di moneta elettronica. In definitiva, le monete elettroniche non sono che la rappresentazione in forma digitale delle valute "tradizionali" a corso legale. Esse fanno riferimento ad un credito verso banche o soggetti vigilati specializzati come emittenti di moneta elettronica e il valore memorizzato elettronicamente è, appunto, un valore "monetario", cioè espresso in una unità di conto avente corso legale[105]. La moneta elettronica deve poter uscire in qualsiasi momento dal circuito dematerializzato e consentire a chi la detiene di entrare in possesso di denaro contante. La stessa direttiva 2009/110/CE, agli artt. 2, n. 2 e 11, prevede espressamente che la moneta elettronica possa essere emessa in cambio di fondi di valore corrispondente emessi in valuta elettronica e debba essere riconvertibile/rimborsabile in valuta reale a richiesta del detentore.

[104] L'art. 1, co. 2, lett. h-*ter*) del T.U.B. è stato modificato dall'art. 1 d.lgs. 16 aprile 2012, n. 45, di attuazione della direttiva 2009/110/CE.
[105] DE STASIO V., *Verso un concetto europeo di moneta legale: valute virtuali, monete complementari e regole di adempimento*, in *Banca borsa*, 2018, n. 6, p. 747 ss., p. 753.

3.5. Le criptovalute.

Diverse dalle monete elettroniche sono le criptovalute. Queste ultime non fanno riferimento al concetto di "moneta", rappresentando soltanto un "valore" idoneo ad essere utilizzato come "mezzo di scambio", dato che non sono emesse da parte della banca centrale o di un soggetto pubblico e non adempiono, in nessun Paese, la funzione di "unità di conto".

Ad oggi non esiste alcuna definizione legale di moneta, né a livello nazionale né sovranazionale[106]. La Banca Centrale Europea ha però espressamente negato che le criptovalute possano definirsi tali, dato che non possiedono in modo completo i tre requisiti affinché una moneta possa dirti tale: non deperibilità, scarsità e divisibilità[107].

Sebbene le valute virtuali abbiano un valore e un mercato, ciò non basta a qualificarle come "moneta", dato che sono prive di un apparato normativo che ne stabilisca la funzione di mezzo di adempimento delle obbligazioni pecuniarie. Le criptovalute sono monete c.d. alternative o private, adottate in un particolare contesto o comunità per fornire un'alternativa rispetto ai sistemi di pagamento esistenti, senza l'emissione e il controllo da parte di una banca centrale[108]. Il rischio maggiore ad esse connesso è l'estrema volatilità, dovuta sia alle fluttuazioni dei prezzi che all'instabilità del mercato[109].

La qualificazione giuridica delle criptovalute è, a tutt'oggi, molto controversa: per alcuni costituiscono mezzi di scambio o strumenti di pagamento[110], per altri beni[111] o

---

[106] MAUME P., MAUTE L., FROMBERGER M., *Rechtshandbuch Kryptowerte. Blockchain, Tokenisierung, Initial Coins Offering*, München, 2020, p. 367.

[107] European Central Bank, *Virtual currency schemes – A further analysis*, 2015, p. 23, disponibile al sito https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf.

[108] LEMME G., PELUSO S., *Criptomoneta e distacco dalla moneta legale: il caso* bitcoin, in *Riv. dir. banc*., 2016, n. 4, p. 381 ss., p. 387.

[109] BRZESZCZYŃSKI, J., GAJDKA J., SCHABEK T., *Bitcoin as a New Currency*, in *Folia Oecon.*, 2020, vol. 20, n. 2, p. 49 ss., p. 62 s.; CORBET S., LUCEY B., URQUHART A., YAROVAYA L., *Cryptocurrencies as a financial asset: A systematic analysis*, in *Int. Rev. Financial Anal.*, 2019, vol. 62, p. 182 ss., p. 19; YI S., XU Z., WANG G., *Volatility connectedness in the cryptocurrency market: Is Bitcoin a dominant cryptocurrency?*, in *Int. Rev. Financ. Anal.*, 2018, vol. 60, p. 98 ss., p. 112.

[110] CIAN M., *La criptovaluta. Alle radici dell'idea giuridica di denaro attraverso la tecnologia: spunti preliminari*, in *Banca borsa*, 2019, n. 3, p. 315 ss., p. 331; ROSEMBERGER P., *Bitcoin und Blockchain. Vom Scheitern einer Ideologie und dem Erfolg einer revolutionären Technik*, Berlin, 2018, p. 15. Si tratterebbe di un mezzo di scambio anche per il Financial Action Task Force (FAFT-GAFI), organizzazione intergovernativa fondata nel 1989, su iniziativa del G7, per sviluppare politiche di contrasto al riciclaggio di denaro. Sul punto v. FATF, *Guidance for a Risk-based approach. Virtual currencies*, 2015, p. 26, disponibile *online* al sito https://www.fatf-gafi.org/documents/documents/guidance-rba-virtual-currencies.html.

[111] CALONI A., *Bitcoin: profili civilistici e tutela dell'investitore*, in *Riv. dir. civ*., 2019, n. 1, p. 159 ss., p. 170; MONTI A., *Per un'analisi critica della natura giuridica delle criptovalute*, in *Rag. prat*., 2018, n. 2, p. 361 ss., p. 371; SIXT E., *Bitcoins und andere dezentrale Transaktionssysteme. Blockchains als Basis einer Kryptoökonomie*, Wiesbaden, 2017, p. 121. Per BOCCHINI R., *Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche*, in *Dir. inf. inf.*, 2017, n. 1, p. 27 ss., p. 33 s., le criptovalute potrebbero essere inquadrate alla stessa stregua di un documento informatico recante dati ed informazioni giuridicamente rilevanti e sottoscritto da una progressione di firme elettroniche, in tal senso v.

strumenti finanziari[112]. Nonostante la mancanza di un ente o soggetto centrale che ne controlli l'emissione, vi è chi riconosce loro la natura di moneta[113]. In ogni caso, va evidenziato che il concetto di riserva di valore non è un connotato esclusivo della moneta, dato che ogni strumento finanziario, ogni merce, ogni bene economico costituisce una riserva di valore[114]. È indubbio, quindi, che le criptovalute abbiano comunque un valore economico. Inoltre, in molti casi è attualmente possibile acquisire criptovalute scambiandole con valuta standard[115].

Il legislatore europeo al punto n. 18 della direttiva 2018/843/UE del Parlamento Europeo e del Consiglio del 30 maggio 2018, che modifica la direttiva 2015/849/UE, relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo, definisce le criptovalute come «*una rappresentazione di valore digitale che non è emessa o garantita da una banca centrale o da un ente pubblico, non è necessariamente legata a una valuta legalmente istituita, non possiede lo status giuridico di valuta o moneta, ma è accettata da persone fisiche e giuridiche come mezzo di scambio e può essere trasferita, memorizzata e scambiata elettronicamente*». Il nostro legislatore ha recepito tale direttiva col d.lgs. 4 ottobre 2019, n. 125, inserendo all'art. 1, lett. qq), d.lgs. 21 novembre 2007, n. 231, la nuova definizione di valuta virtuale, quale «*la rappresentazione digitale di valore, non emessa né garantita da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi o per finalità di investimento e trasferita, archiviata*

[112] MASI D., *Le criptoattività: proposte di qualificazione giuridica e primi approcci regolatori*, in *Banca impresa soc.*, 2021, n. 2, p. 241 ss., p. 255; BAUR D.G., HONG K., LEE A.D., *Bitcoin: Medium of exchange or speculative assets?*, in *J. Int. Financial Mark. Inst. Money*, 2018, vol. 54, p. 177 ss., p. 187.; AA.VV., *Bitcoin - Asset or Currency? Revealing Users' Hidden Intentions*, in *European Conference on Information Systems* - Tel Aviv, 2014, p. 13 e YERMACK D., *Is Bitcoin a real currency? An economic appraisal*, in *NBER Working Paper No. 19747*, 2014, p. 16 s., disponibile al sito https://www.nber.org/papers/w19747. Cft. Corte di Giustizia UE, sentenza 22 ottobre 15, causa C-264/14, Skatteverket c/ David Hedqvist, la quale, pronunciandosi in merito al *Bitcoin*, al par. 49, ha statuito che «*le operazioni relative a valute non tradizionali, vale a dire diverse dalle monete con valore liberatorio in uno o più paesi, costituiscono operazioni finanziarie in quanto tali valute siano state accettate dalle parti di una transazione quale mezzo di pagamento alternativo ai mezzi di pagamento legali e non abbiano altre finalità oltre a quella di un mezzo di pagamento*». In giurisprudenza v. anche Tribunale di Verona, sez. II, sentenza 24 gennaio 2017, n. 195. Dall'analisi relativa alle preferenze degli utenti, la più nota delle valute virtuali, ovvero *Bitcoin*, viene prevalentemente acquistata a fini speculativi o di investimento e solo una minoranza degli utenti, la utilizza come mezzo di scambio.

[113] HAZLETT P. H., LUTHER W. J., *Is bitcoin money? And what that means*, in *Q. Rev. Econ. Finance*, 2020, vol. 77, p. 144 ss., p. 148; MECENATE A., *Il deposito del prezzo in criptomonete presso il notaio*, in *Riv. notariato*, 2021, n. 2, p. 385 ss., p. 394; PLASSARAS N. A., *Regulating Digital Currencies: Bringing Bitcoin within the Reach of IMF*, in *Chi. J. Int'l. L.*, 2013, vol. 14, no. 1, pp. 377 ss., p. 407. Per DHYRBERG A.H., *Bitcoin, gold and the dollar. A GARCH volatility analysis*, in *Finance Research Letters*, 2016, vol. 16, p. 85 ss., p. 92 le criptovalute sarebbero «*somewhere in between a currency and a commodity*».

[114] DE STASIO V., *Verso un concetto europeo*, cit., p. 754.

[115] MASI D., *Le criptoattività*, cit., p. 246.

e negoziata elettronicamente». Tale definizione si differenzia rispetto a quella fornita dal legislatore europeo perché aggiunge espressamente la finalità di investimento. Tale discrasia non è certo di aiuto per l'identificazione della natura giuridica di tali strumenti.

Di recente è stata introdotta nel nostro ordinamento una definizione ai fini penali di valute virtuali dall'art. 1 d.lgs. 8 novembre 2021, n. 184, di attuazione della direttiva 2019/713/UE, relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti. Tale definizione coincide con quella di cui all'art. 2, lett. d), della direttiva 2019/713/UE. La definizione di cui alla direttiva 2019/713/UE volta, coincide con quella fornita dal legislatore europeo nella citata direttiva 2018/843/UE, che però, come sopra esaminato, diverge da quella contenuta nella legge nazionale di attuazione. Ad oggi, dunque, nella nostra normativa interna esistono due diverse definizioni di valuta virtuale, una ai fini della legge penale, ed identica alle definizioni fornite in ambito europeo, e l'altra contenuta nella normativa antiriciclaggio. Inopportuna pare la scelta di prevedere una definizione valida "ai soli effetti della legge penale", dato che le valute virtuali rientrano in un complesso ben più ampio di regolamentazioni extrapenali[116]. Più corretto sarebbe stato prevedere un'unica definizione, identica a quella di cui alle due direttive sopra menzionata.

Il numero di criptovalute esistenti ha già superato le milleseicento unità[117]. La criptovaluta più famosa, e quella che svolge un ruolo dominante, è il *Bitcoin*[118]. Essa si basa su un sistema *peer to peer* puro, in cui ciascun utente ha diritti pari a quelli degli altri, senza che vi sia un'autorità centrale con diritti di gestione della moneta e gli utenti interagiscono tra loro in modo diretto e anonimo, senza intermediari. È, dunque, il solo algoritmo *software* di creazione a definirne le caratteristiche ed i limiti di emissione.

Bitcoin, come altre criptovalute, è strutturalmente legata alla tecnologia *blockchain*[119]. Quest'ultima è controllata e generata sfruttando i principi base della

---

[116] PICOTTI L., *«Nuovi» crimini cibernetici e possibile rilevanza penale dell'intelligenza artificiale. (Atti digitali del convegno gli Stati Generali del diritto di Internet*, Luiss, 16,17,18 dicembre 2021), in *Diritto di Internet*, 2022, supplemento al n. 1, p. 1 ss., p. 11.

[117] YI S., XU Z., WANG G., *Volatility connectedness*, cit., p. 98.

[118] *Bitcoin* fu creata nel 2009 da uno o più programmatori sotto lo pseudonimo di Satoshi Nakamoto. Sulla sua reale identità sono state fatte moltissime ipotesi e l'identità del creatore di *bitcoin* è stata negli anni attribuita a varie persone: dall'informatico Nick Szabo, a un collezionista giapponese di modellini di treni, fino all'australiano Craig Steven Wright, che ancora oggi sostiene di essere la persona dietro lo pseudonimo. Altre fonti sostengono che Satoshi Nakamoto non sia una persona, ma piuttosto un acronimo per le società per le aziende Samsung, Toshiba, Nakamichi e Motorola.

[119] *Blockchain* significa letteralmente "catena di blocchi" e rappresenta un particolare utilizzo della *Distributed Ledger Technology*, ovvero "libri mastri" (o registri) elettronici, distribuiti geograficamente su un'ampia rete di nodi, i cui dati sono protetti da potenziali attacchi informatici grazie al fatto che le stesse informazioni sono ridondate, verificate e validate mediante l'adozione di diversi protocolli comunemente accettati da ciascun partecipante. Si chiama *distributed* proprio perché non è presente un'autorità centrale col compito di validare le transazioni. Per approfondire v.: OMOTE K., YANO M., *Bitcoin and Blockchain Technology*, in C. Dai, K.

crittografia attraverso l'algoritmo di un *software* libero, non protetto da *copyright*, ovvero un *network* decentralizzato o *peer-to-peer*, per cui ciascun utente è sia fruitore che distributore delle informazioni di rete. In tale sistema gli attori principali sono costituiti dagli utenti (*users*), dai nodi (*nodes*), dai "minatori" (*miners*) e dagli sviluppatori (*devs*)[120]. Vi è un registro organizzato in "blocchi" individualmente identificabili, che raggruppano insiemi di transazioni in essi registrate, tra loro collegati in modo da formare una "catena" sequenziale marcata temporalmente.

Lo scambio tra le transazioni è reso possibile grazie a un *database* distribuito tra i nodi della rete Internet, i quali tengono traccia di tutte le transazioni e le verificano. Ogni blocco è dotato di un *header*, utilizzato per organizzare il database distribuito, il quale, a sua volta, contiene l'*hash* (ovvero una sorta di impronta digitale) di tutte le transazioni registrate nel blocco, la marcatura temporale (*timestamp*) e l'*hash* del blocco precedente, che consente la ricostruzione (anche cronologica) della catena di blocchi. L'integrità del sistema è assicurata dal fatto che gli *hash* non vengono generati automaticamente, ma solo all'esito di una particolare procedura che richiede l'impiego di risorse computazionali per risolvere un certo algoritmo matematico.

I nodi del *network* sono in competizione tra loro per la generazione di *hash* di chiusura di ciascun blocco della catena ed il primo che riesce a risolvere tale algoritmo, dando prova di aver impiegato risorse per raggiungere tale scopo (c.d. *proof of work*) comunica la soluzione nel *network*, che verrà verificata dagli altri nodi. Se la soluzione comunicata è corretta, il blocco è aggiunto alla *blockchain* e salvato su tutti i nodi partecipanti al network[121]. In tal modo il *network* raggiunge il consenso sull'ammontare di valore posseduto da ciascuno dei partecipanti e la presenza nel blocco dell'*hash* del blocco precedente rende il tentativo di modifica di un blocco già registrato pregiudizievole dell'intera catena, in quanto darebbe luogo alla modifica dell'*hash* di tale blocco ed a quella di tutti i successivi[122].

Masuda, Y. Kishimoto (eds.), *Blockchain and cryptocurrency. Building a High Quality Marketplace for Crypto Data*, Singapore, 2020, p. 129 ss.; GAYVORONSKAYA T., MEINEL C., *Blockchain. Hype or innovation*, Cham, 2021, p. 15 ss.; PORXAS N., CONEJERO M., *Tecnología blockchain: funcionamento, aplicaciones y retos jurídicos relacionados*, in *Act. jur. Uría Menéndez*, 2018, n. 48, p. 24 ss. Il funzionamento di *Bitcoin* è stato reso noto dal suo stesso creatore tramite la pubblicazione di un documento nella forma di *white paper*. V. NAKAMOTO S., *Bitcoin: a Peer-to-Peer Elettronic Cash System*, 31 ottobre 2008, disponibile *online* al sito https://bitcoin.org/bitcoin.pdf.

[120] CAPACCIOLI S., *Storia e tecnica*, in ID (a cura di), *Criptoattività, criptovalute e bitcoin*, Milano, 2021, p. 14.

[121] ROSEMBERGER P., *Bitcoin und Blockchain*, cit., p. 66.

[122] OMOTE K., YANO M., *Bitcoin and Blockchain Technology*, cit., p. 132.

La fiducia verso l'emittente assume un ruolo molto importante, perché manca un ente deputato alla verifica della correttezza delle transazioni. La tecnologia *blockchain* si basa sul presupposto che la maggior parte della potenza di calcolo (non degli utenti), sia nelle mani di operatori onesti[123]. Ogni operazione deve essere approvata dal cinquanta per cento più uno dei nodi della catena *blockchain*[124].

Non è possibile possedere *Bitcoin* al di fuori della *blockchain*. Si possono possedere solo indirizzi della *blockchain*, che danno il diritto a "spendere" o "ottenere" *Bitcoin*. I *Bitcoin*, infatti, sono unici e non possono essere duplicati; esistono solo come univoca informazione elettronica[125]. Gli unici che possono ottenere nuovi *Bitcoin* sono i *miners*, vale a dire gli estrattori che esercitano l'attività di *mining*, ma possono farlo solo in maniera fissa e predicibile. Essi utilizzano la propria potenza di calcolo per individuare e verificare le soluzioni dell'algoritmo crittografico posto a base del sistema[126].

L'offerta di nuovi *Bitcoin* è, quindi, indissolubilmente legata al processo di *mining*, il cui svolgimento viene ricompensato con l'attribuzione di unità di nuova moneta virtuale, generate e attribuite all'operatore che per primo riesce a risolvere il complesso calcolo di validazione di un blocco di transazioni. Il meccanismo del *mining* è andato modificandosi nel tempo. Mentre in origine era possibile prendere parte alla procedura di validazione in maniera autonoma, oggi l'attività di *mining* viene in larga parte svolta da utenti associati in *pool* sempre più grandi, i quali condividono la propria capacità elaborativa e in base a questa si ripartiscono le relative ricompense.

I *Bitcoin* possono essere acquistati con denaro avente corso legale oppure possono essere ottenuti all'esito di una transazione per la vendita di beni o servizi[127]. In generale tutte le criptovalute sono (direttamente o indirettamente) convertibili in denaro. *Bitcoin*, *Ethereum* o *Litecoin* possono essere direttamente convertite; per altre, invece, è necessario il previo scambio con una tipologia di criptovalute direttamente convertibili[128].

Bitcoin non ha alcun supporto fisico, per cui dev'essere memorizzata in portafogli, i c.d. *wallet*. Esistono diverse tipologie di *wallet*: gli *hardware-wallet*, installati su appositi

---

[123] GAYVORONSKAYA T., MEINEL C., *Blockchain*, cit., p. 7; PASS R., SEEMAN L., SHELAT A., *Analysis of the blockchain protocol in asynchronous networks*, in Coron J.S., Buus Nielsen J. (eds.), *Advances in* Cryptology. EUROCRYPT 2017. 36th *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Cham, 2017, p. 643 ss., p. 644.
[124] BOCCHINI R., *Lo sviluppo della moneta virtuale*, cit., p. 38.
[125] YERMACK D., *Is Bitcoin a real currency?*, cit., p. 17.
[126] BOCCHINI R., *Lo sviluppo della moneta virtuale*, cit., p. 38.
[127] MASI D., *Le criptoattività*, cit., p. 247.
[128] DASKALAKIS N., GEORGITSEAS P., *An introduction to Cryptocurrencies. The Crypto Market Ecosystem*, London, 2020, p. 27.

dispositivi, i *desktop-wallets,* che vengono memorizzati localmente mediante apposito *software* sul *deskstop*, i *mobile-wallets,* su dispositivi elettronici, ad esempio, *smartphone* o *tablet*, i *paper-wallets*, che consistono nella stampa dei due codici QR contenenti l'indirizzo pubblico per ricevere la chiave privata memorizzare e trasferire i *Bitcoin*. Vi sono, infine, gli *online-wallets,* portafogli *online* la cui gestione è demandata a specifici gestori che offrono questo tipo di servizio, c.d. *wallet providers*[129]. La particolarità di questi ultimi è che l'utente non dispone delle transazioni che effettua, ma richiede al gestore dell'*online-wallet* di effettuarle[130].

La quantità di *Bitcoin* in circolazione è limitata a priori ed è, dunque, perfettamente prevedibile da tutti gli utenti[131].

La questione circa l'anonimato delle transazioni effettuate nello schema *Bitcoin* è tuttora oggetto di un ampio dibattito. Le transazioni in *Bitcoin* sono totalmente anonime, perché non richiedono nessuna informazione personale per essere portate a compimento[132]. A differenza dell'apertura di un conto corrente bancario, per prendere parte al procedimento di creazione delle criptovalute o di loro acquisti non è necessario presentare alcun documento di identità ed è possibile per gli utenti rimanere anonimi. Il c.d. libro mastro della *blockchain* è pubblico e può essere liberamente visualizzato. Anche se i pagamenti sono criptati, sono tutti tracciabili sulla *blockchain*. In tal senso, una parte della dottrina preferisce parlare di pseudoanonimato[133], piuttosto che di anonimato vero e proprio.

Alcuni esperti negano che la tecnologia *blockchain* consenta un anonimato totale[134]. Nell'ambito della *computer forensics* sono già state sviluppate tecniche per tracciare e localizzare l'utilizzo di *criptovalute* da parte di un indagato, per cui è possibile tracciare l'indirizzo IP utilizzato nelle transazioni e addirittura ricostruire il collegamento col *Service Provider* che opera come cambiavalute[135]. Non si tratterebbe, dunque, di un sistema

[129] ROSEMBERGER P., *Bitcoin und Blockchain,* cit., p. 22 ss.
[130] CAPACCIOLI S., *Storia e tecnica*, cit., p. 66.
[131] LEMME G., PELUSO S., *Criptomoneta,* cit., p. 396.
[132] *Ibid*., p. 400.
[133] MAUME P., MAUTE L., FROMBERGER M., *Rechtshandbuch Kryptowerte,* cit., p. 28.
[134] Un recente studio del Politecnico di Milano ha dimostrato che le transazioni *Bitcoin* non sono totalmente e sistematicamente anonime, per cui tramite l'utilizzo di determinati strumenti, partendo dai registri delle transazioni è possibile risalire ad un gran numero di informazioni sull'identità di un soggetto fino a collegarne l'attività a fatti specifici, di interesse investigativo. In argomento v. SPAGNUOLO M., MAGGI F., ZANERO S., *Bitiodine: Extracting intelligence from the bitcoin network* in Christin N., Safavi-Naini R. (eds.), *International Conference on Financial Cryptography and Data Security*, Berlin, 2014, pp. 457 ss.
[135] MONTI A., *Per un'analisi*, cit., p. 374.

anonimo[136]. Tuttavia, tale procedura è abbastanza complessa e gli ostacoli pratici per le forze dell'ordine per risalire all'identità del proprietario dei *Bitcoin* sembrano ancora rilevanti[137]. Il problema della tracciabilità può essere, almeno in parte, aggirato prendendo le opportune precauzioni, ovvero utilizzando nuovi indirizzi per l'invio di pagamenti e per ogni pagamento ricevuto o avvalendosi degli appositi servizi offerti da c.d. *mixer* o *tumbler*. Si tratta di soggetti che vengono ingaggiati per nascondere ogni traccia di collegamento tra l'utente-cliente e i *Bitcoin* da questi posseduti o trasferiti[138]. I *mixer* o *tumbler* posseggono numerose chiavi pubbliche e trasferiscono in modo casuale e automatico i *Bitcoin* provenienti dai loro clienti. I *Bitcoin* possono essere scambiati con i *Bitcoin* di altri utenti, suddivisi tra diversi indirizzi di destinazione e trasferiti a intervalli casuali per rendere più difficile stabilire connessioni a causa di correlazioni temporali o importi congruenti[139].

L'anonimato o lo pseudoanonimato non è identico per tutte le criptovalute. *Monero*, per esempio, è estremamente orientata verso la *privacy* degli utilizzatori: il *wallet* che la supporta non richiede alcuna informazione personale per la sua emissione[140]. Per i soggetti diversi da quelli coinvolti nella transazione non è inoltre possibile consultare né gli indirizzi coinvolti nella transazione né l'importo della stessa. La questione dell'anonimato delle criptovalute, dunque, è molto più complessa di quanto appare ed è ben lontana da un'univoca soluzione.

3.6. I *token*.

Diversi dalle criptovalute sono i *token*. Questi ultimi non sono parte integrante della tecnologia *blockchain*, ma sono beni digitali, che operano sfruttando *blockchain* esistenti e possono rappresentare qualsiasi bene di valore, non necessariamente la valuta virtuale sulla cui *blockchain* sono registrati[141].

Le regole alla base di un *token* sono sancite in uno *smart contract*, ovvero un programma archiviato sulla *blockchain*, la quale registra anche le transazioni effettuate con quel *token*. Gli *smart contract* non sono contratti nel vero senso della parola, ma *software*

---

[136] SICIGNANO G.J., *Money Laundering Using Cryptocurreny*, in *Athens JL*, 2021, vol. 2, n. 7, p. 253 ss., p. 256.
[137] BUSSMAN K.D., *Geldwäscheprävention im Markt - Funktionen, Chancen und Defizite*, 2018, Berlin, p. 138.
[138] LEMME G., PELUSO S., *Criptomoneta*, cit., p. 401.
[139] GRZYWOTZ G., KÖHLER O.M., RÜCKERT C., *Cybercrime mit Bitcoins – Straftaten mit virtuellen Währungen, deren Verfolgung und Prävention*, in *StV*, 2016, n. 11, p. 753 ss., p. 755.
[140] CAPACCIOLI S., *Storia e tecnica*, cit., p. 76 s.
[141] HÖNIG M., *ICO und Kryptowährungen. Neue digitale Formen der Kapitalbeschaffung*, Wiesbaden, 2020, p. 34.

per l'esecuzione automatica del *token*[142]. Essi agiscono in modo automatico, secondo le condizioni prestabilite dalle parti e poi tradotte in un codice informatico. Normalmente essi prevedono il trasferimento di criptovaluta, quale corrispettivo di una determinata obbligazione. La loro peculiarità è l'irreversibilità: una volta che essi sono stati iscritti nella *blockchain* non possono essere risolti, finché non venga adempiuta la prestazione dedotta[143].

Vi sono diverse tipologie di *token*. Per *currency token* si intendono i *token* con funzione di mezzo di scambio[144]. Vi sono poi gli *investment token*, ossia i *token* con funzione di investimento, che offrono diritti di partecipazione agli utili futuri dell'emittente, diritto ad un pagamento fisso oppure un diritto di partecipazione. Si pensi ad esempio agli *equity token*, che non sono altro che *token* di investimento collegati alle azioni di una società, così come i *security token*, la cui funzione è quella di conferire al proprietario una partecipazione agli utili di una società, o una quota della stessa o qualche altra forma di ricompensa, e che sono comunque connessi con la proprietà di un bene già esistente. Gli *utility token* forniscono ai titolari l'accesso ad un determinato di un determinato prodotto o servizio[145]. Spesso vengono utilizzati come *voucher* o buono sconto per l'acquisto di quel prodotto o servizio. Si differenziano dai *security token* perché non possono essere utilizzati quali strumenti finanziari[146]. Diversi sono i *commodity token*, che consistono in una tipologia di *token* garantita da beni specifici già esistenti, ovvero i c.d. *commodity* o prodotti primari di scambio[147]. I *non fungible token* o NFT, per cui *non fungible* non possono essere sostituiti, trattandosi di una rappresentazione digitale di un bene regolata da uno *smart contract* e commercializzabile in criptovalute. Essi consentono la proprietà di artefatti unici, quali, ad esempio, un'immagine, un'animazione, una foto, un *avatar*, un *videoclip*, ecc., che sono autenticati e rintracciabili nella *blockchain*[148].

---

[142] EBERS M., HEINZE C., KRÜGEL T., STEINRÖTTER B. (Hrsg.), *Künstliche Intelligenz und Robotik*, München, 2020, p. 400.
[143] ACCINNI G., *L'utilizzo criminogeno della* blockchain*: gli* smart contract, in *Sist. pen*., 2022, n. 6, p. 133 ss., p. 134.
[144] MAUME P., MAUTE L., FROMBERGER M., *Rechtshandbuch Kryptowerte*, cit., p. 19.
[145] *Ibid*., p. 20.
[146] HÖNIG M., *ICO und Kryptowährungen*, cit., p. 35 ss.
[147] Una *commodity* viene definita come «*A raw material traded on a commodity market, such as grain, coffee, cocoa, wool, cotton, jute, rubber, pork bellies, or orange juice (sometimes known as soft commodities) or metals and other solid raw materials (known as hard commodities). In some contexts soft commodities are referred to as produce*», (v. voce *commodity* in LAW J. (eds.), *A Dictionary of Finance and Banking*, cit.).
[148] CHANDRA Y., *Non-fungible token-enabled entrepreneurship: a conceptual framework*, in *J. Bus. Ventur. Insights*, 2022, n. 18, p. 1 ss., p. 1.

4. Le minacce cibernetiche al patrimonio e l'utilizzo illecito dell'intelligenza artificiale per fini patrimoniali: tasso di incidenza, dimensioni dei nuovi fenomeni criminosi e *modus operandi* dei *cybercriminali*.

Nella società odierna, gli attacchi informatici diretti contro il patrimonio costituiscono un fenomeno in rapida espansione. A causa dell'emergenza sanitaria da Covid-19 e il conseguente maggiore utilizzo dei servizi Internet, nel corso del 2020 vi è stato un aumento esponenziale nella commissione di truffe e frodi commesse sul *web*, in controtendenza rispetto alla generale diminuzione dei reati perpetrati[149]. Nel primo trimestre del 2022 si è raggiunta la cifra record di 1.025.968 attacchi di *phishing*, la cifra più alta di attacchi informatici mai registrata finora in un solo quadrimestre[150]. Questo dato è da solo sufficiente per comprendere la dimensione del fenomeno. In realtà, il numero effettivo di cyberattacchi è molto più alto e si stima che ogni giorno vengano creati da trecentomila ad un milione di nuovi virus informatici[151].

Gli attacchi informatici non coinvolgono solo i singoli individui, ma anche le infrastrutture critiche, tra cui ospedali. Nell'ultimo anno gli attacchi *ransomware* diretti contro infrastrutture critiche sono aumentati del 40%[152].

Negli ultimi anni i criminali informatici hanno notevolmente perfezionato le loro tecniche e gli attacchi informatici sono diventati molto sofisticati. La crescita esponenziale degli attacchi informatici è principalmente dovuta alla disponibilità di tecnologie sempre più sofisticate da parte dei *cybercriminali*, il crescente utilizzo del *web* da parte di nuovi utenti poco esperti, spesso residenti in Paesi ove la sicurezza delle infrastrutture digitali è trascurata, si aggiunge alla possibilità di monetizzare facilmente i dati e *file* illecitamente intercettati[153].

Gli attacchi informatici contro il patrimonio garantiscono la possibilità di lauti guadagni a fronte di scarsissime probabilità di incorrere in sanzioni, dato che le autorità di *law enforcement* non sempre posseggono strumenti tecnologici all'avanguardia al pari dei criminali informatici e, quindi, non riescono a risalire all'origine e all'identità

[149] V. i dati raccolti nel 2020 dalla Polizia di Stato e diffusi nell'aprile 2021 in occasione del 169° anniversario della fondazione della Polizia di Stato, disponibile al sito https://poliziamoderna.poliziadistato.it.
[150] Anti Phishing Working Group, *Phishing Activity Trends Report. Unifying the Global Response to Cybercrime. 1st Quarter 2022*, 2022, disponibile *online* al sito www.apwg.org, p. 3.
[151] LEWIS J., *Economic Impact of Cybercrime—No Slowing Down*, *Report* per Center for Strategic and International Studies e McAfee, 2018, p. 4, disponibile al sito https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf.
[152] Dati raccolti nel *Report* a cura dell'azienda SoSafe, *Human Risk Review 2021. An Analysis of the European Cyberthreat Landscape*, 2021, disponibile all'indirizzo https://sosafe-awareness.com/resources/reports/human-risk-review/.
[153] LEWIS J., *Economic Impact of Cybercrime*, cit., p. 6.

dell'attaccante[154]. I criminali informatici hanno spesso la possibilità di agire al di là dei confini nazionali, senza necessità di avere un contatto fisico con il sistema da attaccare, per cui possono dirigere i loro attacchi *hacker* contro soggetti o istituzioni situate in Paesi ove manca un quadro giuridico adeguato a reprimere tali fenomeni[155].

Il fenomeno del *cybercrime* ha ormai assunto portata internazionale ed è oggi una delle principali sfide che la comunità internazionale è chiamata ad affrontare. Nel *ranking* del *Word Economic Forum* la criminalità informatica è indicata come la terza più grande minaccia per l'economia globale[156]. Gli attacchi informatici avvengono su larga scala, a volte addirittura a livello globale. Le perdite finanziarie i derivanti dagli attacchi informatici sono ingenti e sono state stimate in un trilione di dollari per il 2020 e in sei trilioni per il 2021[157].

Nonostante le conseguenze lesive del fenomeno, che coinvolge sempre più anche i sistemi informatici dello Stato, i criminali informatici responsabili di tali attacchi vengono effettivamente perseguiti penalmente in un numero molto limitato di casi. A tal proposito, è sufficiente rilevare che su oltre 196mila segnalazioni pervenute alle forze dell'ordine italiane relativamente alla commissione di frodi e reati informatici nel 2019, l'autore dei reati è stato individuato solo nel 3,1% dei casi. Del tutto marginale, poi, è l'incidenza delle frodi informatiche nelle statistiche giudiziarie italiane relative alle condanne, tant'è che non vengono neppure inserite in una categoria a sé stante, bensì indicate alla voce "*altri reati*"[158]. Il motivo principale del basso numero di condanne a fronte della commissione di un elevato numero di frodi è che le indagini in quest'ambito sono particolarmente complicate, dato che i criminali informatici utilizzano *software* o reti VPN (*Virtual private network*) che ne nascondono l'identità.

Va poi evidenziato che di fronte all'evoluzione e dell'espansione del *cyberspace* è mutato anche l'approccio alla criminalità informatica, che comprende una molteplicità di illeciti e non è più riconducibile ad un numero circoscritto di reati. Le minacce cibernetiche che verranno meglio descritte (v. *infra*, par. 5 e ss.) sono tutte manifestazioni del più ampio del fenomeno del *cybercrime,* contrapposto al *computer crime,* perché si tratta di un evento

---

[154] *Ibid.*, p. 4.

[155] TROPINA T., *Organized Crime in Cyberspace*, in H. Böll-Stiftung e R. Schönenberg (eds.), *Transnational Organized Crime. Analyses of a Global Challenge to Democracy*, Bielefeld, 2013, p. 47 ss., p. 48.

[156] V. World Economic Forum, *COVID-19 has disrupted cybersecurity, too - here's how businesses can decrease their risk*, 2020, disponibile *online* all'indirizzo https://www.weforum.org/agenda/2020/07/covid-19-cybersecurity-disruption-cyber-risk-cyberattack-business-digital-transformation/.

[157] CLUSIT (Associazione italiana per la sicurezza informatica), *Rapporto 2021 sulla Sicurezza ICT in Italia*, Milano, 2021, p. 7, consultabile al sito www. clusit.it/pubblicazioni/.

[158] V. dati dell'Istituto Nazionale di statistica relativi all'anno 2019 con riguardo alla tipologia di reati commessa, ai delitti di cui si è scoperto l'autore e dei condannati con riferimento alla natura del reato, disponibili *online* al sito «http://dati.istat.it».

lesivo commesso in rete avvalendosi della stessa rete *Internet.* I reati cibernetici (o reati informatici "in senso ampio") sono infatti tutti quelli che vengono commessi nel *cyberspace,* espressione volta ad indicare sia di nuove forme di condotte illecite sia la commissione di reati tradizionali per mezzo della rete*,* mentre i *computer crime,* o reati informatici "in senso stretto", sono quelli compiuti a mezzo del *computer,* ovverosia: quelli che nella fattispecie legale contengono un elemento tipizzato che riguarda l'informatica; quelli ove l'informatica costituisce la modalità di compimento del reato; oppure quelli ove l'informatica riguarda l'oggetto del reato rientrando in questo modo nella fattispecie penale[159]. A venire in rilievo, dunque, non sono unicamente i reati informatici, ma anche fattispecie tradizionali. Come si esaminerà nel prosieguo, questo è un ulteriore elemento di complicazione in un sistema caratterizzato da un lato da sovrabbondanza di fattispecie penali, ma dall'altro da sorprendenti vuoti di tutela.

4.1. Le cyber-organizzazioni criminali.

Se agli albori del fenomeno gli *hacker* erano adolescenti o comunque singoli individuati con elevata o media competenza informatica, che volevano sperimentare le loro capacità informatiche e guadagnare qualche soldo[160], oggi sono spesso componenti di associazioni a delinquere che operano su scala mondiale[161]. Gli studiosi distinguono tra la criminalità organizzata tradizionale che opera anche sul *web* ed i gruppi organizzati dediti esclusivamente alla commissione di reati cibernetici. Nel *cyberspace* operano non soltanto tradizionali associazioni a delinquere, le quali utilizzano Internet come spazio virtuale per i loro traffici illeciti protetti dall'anonimato, ma anche nuove strutture organizzate che operano esclusivamente sul *web*[162]. Quest'ultimo fenomeno è ancora poco studiato e non è

---

[159] La distinzione tra *computer crime* e *cybercrime* con relativo passaggio all' *'"epoca di Internet",* ove il *cyber space* è diventato l'ambiente ideale e privilegiato per la realizzazione di molteplici reati è descritta da Picotti in PICOTTI L., *Sistematica dei reati informatici,* cit., p. 29. Più di recente v. anche PICOTTI L., *Cybercrime e diritto penale,* in C. Parodi, V. Sellaroli (a cura di), *Diritto penale dell'informatica. Reati della rete e sulla rete,* Milano, 2020, p. 709 ss., p. 712.

[160] WILLELMS E., *Cyberdanger. Understanding and Guarding Against Cybercrime,* 2019, Cham, p. 13 evidenzia che il più grande gruppo di creatori di *malware* degli anni '80 (i c.d. *Script Kiddies*) era costituito proprio da adolescenti curiosi di vedere come le loro "creazioni" si sarebbero comportate nel mondo reale.

[161] Già Cajani, Costabile e Mazzarco in CAJANI F., COSTABILE G., MAZZARACO G., *Phishing e furto d'identità digitale. Indagini informatiche e sicurezza bancaria,* Milano, 2008, p.188. riportavano la presenza di diverse organizzazioni criminali appositamente dedite a creare ed inviare *e-mail* di *phishing*.

[162] WANG P., SU M., WANG J., *Organized crime in cyberspace: how traditional organized criminal groups exploit the online peer-to-peer lending market in China,* in *Brit. J. Criminol*., 2021, n. 61, p. 303 ss., p. 303; FLOR R., LUPARIA L., *Criminalità organizzata e criminalità informatica ("cyberorganized crime")*, in *Dir. pen. cont.*, 2019, p. 202 ss., p. 206.

chiaro quanto sia esteso[163]. Negli studi più recenti[164] si è evidenziato che le strutture criminali organizzate non presentano le gerarchie proprie delle associazioni a delinquere di stampo tradizionale, quanto, piuttosto, divisioni per specifici compiti. In tal senso, si distingue tra *core members*, *enablers* e *money mule*: i primi sono i c.d. membri principali, coloro che organizzano e coordinano gli attacchi *hacker* contro determinate istituzioni; gli *enabler* sono coloro che agevolano i compiti dei *core members* fornendo loro *malware*, *password* o altri strumenti utili a realizzare l'attacco informatico, mentre i *money mules* sono coloro che si occupano di nascondere la provenienza illecita del denaro o dei beni illecitamente sottratti dai *core members*[165]. Gli *enabler* non sono sempre presenti e spesso operano per diversi gruppi criminali, promuovendo *online* i loro servizi.

I *money mules*, quando presenti, formano il gruppo più numeroso di partecipanti. Anch'essi vengono reclutati *online* e per occultare la provenienza delittuosa di una singola transazione possono operare in centinaia[166].

Nella maggior parte dei casi i *core members* sono membri stabili, che possiedono determinate competenze tecniche e spesso sono residenti nei c.d. Paesi emergenti del *cybercrime* quali, ad esempio, Brasile, India e Vietnam[167]. Queste nuove strutture criminali si caratterizzano per il loro notevole decentramento e per la richiesta di collaborazione da parte di soggetti estranei[168]. Non mancano strutture organizzate nelle quali i *core members* sono membri di organizzazioni a delinquere tradizionali e già note alle forze dell'ordine, desiderosi di cimentarsi in nuovi redditizi traffici illeciti[169]. Con l'affermarsi del fenomeno del *Cybercrime-as-a-service*, le associazioni a delinquere di stampo tradizionale non necessitano di particolari competenze informatiche e possono operare anche in quest'ambito, moltiplicando i loro guadagni[170]. Ad ogni modo, le nuove strutture criminali presentano l'insieme minimo di caratteristiche per essere considerate organizzazioni criminali, anche se a volte non corrispondono esattamente alle definizioni legislative di criminalità organizzata, in particolare con riferimento agli scopi perseguiti[171].

---

[163] TROPINA T., *Organized Crime in Cyberspace*, cit., p. 47.
[164] RUTGER LEUKFELDT E., LAVORGNA A., KLEEMANS E.R., *Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime*, in *Eur. J. Crim. Policy Res*., 2016, vol. 23, n. 3, p. 287 ss., p. 291.
[165] *Ibid*., p. 292.
[166] *Ibid*.
[167] LEWIS J., *Economic Impact of Cybercrime*, cit., p. 5.
[168] RUTGER LEUKFELDT E., LAVORGNA A., KLEEMANS E.R., *Organised Cybercrime*, cit., p. 293.
[169] *Ibid*.
[170] AA.VV., *Cyber-OC-Scope and manifestation in selected EU member states*, Wiesbaden, 2016, p. 223.
[171] RUTGER LEUKFELDT E., LAVORGNA A., KLEEMANS E.R., *Organised Cybercrime*, cit., p. 297.

4.2. Il *Cybercrime-as-a-service*.

Gli attacchi informatici contro il patrimonio si articolano di regola in più fasi, di cui l'effettivo depauperamento della vittima mediante frode costituisce la fase finale. I criminali informatici per ottenere l'accesso al conto corrente o al denaro della vittima devono prima carpire le sue credenziali, i dati di accesso all'*account* tramite un attacco di tipo *phishing*, *skimming*, ecc.[172]. In tale contesto, si è affermato negli ultimi anni il c.d. *Cybercrime-as-a-service*[173]. Coloro che realizzano la frode informatica non sono i criminali che si sono impossessati delle credenziali o dei dati personali delle vittime, bensì sono soggetti che hanno previamente acquistato tali dati sul *dark web*, ove esiste un vero e proprio "mercato nero" nel quale i dati (personali, i numeri di carte di credito, i PIN, ecc.) delle vittime vengono venduti a loro insaputa[174]. Nel mercato nero globale è possibile acquistare sofisticati strumenti di attacco (quali ad esempio *malware*) ed acquisire conoscenze sulle vulnerabilità di determinati sistemi operativi o di *target*. Gli acquirenti meno esperti possono direttamente acquistare dei c.d. *exploit kit*, ovvero un insieme di *software* che consente di distribuire *malware* e *ransomware* automaticamente[175]. Non è, quindi, più necessario per il criminale informatico possedere specifiche conoscenze tecnico-informatiche. Si può noleggiare una *bootnet*, ovvero una rete di *computer* controllata da un *bootmaster* e composta da dispositivi infettati da un *malware* specializzato denominati *bot*, che possono avere diverse funzioni quali quella di inviare massicce mail di *spam* o di sovraccaricare un *Server*[176].

Del fenomeno del *Cybercrime-as-a-service* fa parte anche l'*Obfuscation-as-a service*, che rappresenta un importante supporto per la criminalità informatica. In questo caso, i criminali informatici, dietro pagamento di un compenso, offrono agli utenti la possibilità di occultare la funzione dannosa di un *file*, facendo in modo che il *malware* non venga rilevato dal sistema antivirus[177]. La peculiarità di questo servizio consiste nel cambiare

---

[172] VAN NGUYEN T., *The modus operandi of transnational computer fraud: a crime script analysis in Vietnam*, in *Trends Organ. Crim.*, 2022, n. 25, p. 226 ss., p. 228.
[173] MANKY D., *Cybercrime as a service: a very modern business*, in *Comput. Fraud secur*., 2013, n. 6, p. 9 ss., p. 9.
[174] V. OECD, *Scoping Paper on Online Identity Theft*, Seul, 2008, disponibile *online* al sito www.oecd.org/dataoecd/35/24/40644196.pdf, p. 22.
[175] FRANOSCH R., *Das Darknet – ein rechtsfreier Raum? Überlegungen zur Notwendigkeit einer Digitalen Agenda für das Straf- und Strafprozessrecht*, in P.E. Sensburg (Hrsg.), *Sicherheit in einer digitalen Welt*, Baden-Baden, 2017, p. 23 ss., p. 26.
[176] WEBER A., *Die Strafbarkeit von Plattformbetreibern im Darknet*, Baden-Baden, 2022, p. 54 s.
[177] ŠEMBERA V., PAQUET-CLOUSTON M., GARCIA S., ERQUIAGA M., *Cybercrime Specialization: An Expose of a Malicious Android Obfuscation-As-A-Service*, in *2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 2021, p. 213 ss., p. 213.

il funzionamento del programma, mantenendone intatta la sua funzionalità, ostacolando l'identificazione delle potenziali funzioni dannose inserite nel programma[178].

4.3. *Dark web*, *Marketplace e Intelligenza artificiale*.

Il *dark web* è il luogo ideale per svolgere affari illeciti: esso non è che una parte del *deep web*, ovverosia la c.d. parte invisibile del *web*, nella quale si trovano contenuti non visibili ai motori di ricerca (quali ad esempio cartelle cliniche, documenti finanziari e altri contenuti che si vogliono mantenere riservati)[179]. Per accedere al *dark web* è necessario utilizzare un *browser* specifico adatto allo scopo (ad esempio *Tor* e *I2P*)[180]. Anche se i *browser* non sono stati creati appositamente per lo svolgimento di attività illecite, grazie all'anonimato e alla possibilità di crittografare i dati che essi garantiscono, diventano lo strumento ideale per la vendita di prodotti o servizi di natura illecita[181].

Al contrario di quanto avviene per il *surface web*, i contenuti del *dark web* non sono liberamente visualizzabili: essi non utilizzano i regolari domini del *web* tradizionale, bensì uno speciale *.onion top-level domain* (c.d. TLD), che funziona solo con quel determinato *browser* ed è costruito in modo tale che solo chi conosce esattamente i sedici caratteri alfanumerici di cui è composto possa accedervi[182].

Nel mercato parallelo del *dark web* si distingue tra *Marketplace*, *Vendorshops*, *Forum* e piattaforme organizzate decentralizzate quali ad esempio *OpenBazaar*[183]. I *Marketplace*, detti anche mercati delle criptovalute, sono orientati all'acquisto o alla vendita di beni. A differenza delle convenzionali piattaforme di commercio *online* essi offrono, però, una gamma di prodotti costituita principalmente da beni e servizi illegali[184].

Tra i beni di provenienza illecita figurano numeri di carte di credito clonate (alle volte con relativo PIN), documenti di identità, codici fiscali e *social security numbers*, credenziali e *password* di utenti ignari. I loro prezzi possono variare in relazione alla loro natura, quantità, Paese di origine e in alcuni casi si effettuano addirittura sconti e promozioni per invogliare gli acquirenti. I *Vendorshops* sono pagine di singoli rivenditori che vendono

---

[178] *Ibid*., p. 214.
[179] AA. VV., *Understanding the Dark Web*, in B. Akhgar, M. Gercke, S. Vrochidis, H. Gibson (a cura di), *Dark Web Investigation*, Cham, 2021, p. 3 ss., p. 5.
[180] *Ibid*., p. 8.
[181] HÖNIG M., *ICO und Kryptowährungen. Neue digitale Formen der Kapitalbeschaffung*, Wiesbaden, 2020, p. 80.
[182] AA. VV., *Understanding the Dark Web*, cit., p. 9.
[183] WÜST M., *Die Underground Economy des Darknets. Die Strafbarkeit des Betreibens „illegaler" Handelsplattformen*, Berlin, 2022, p. 34.
[184] *Ibid*., p. 35.

determinati beni di provenienza illecita[185]. Vi sono poi i *forum*, che servono alla discussione e comunicazione tra gli utenti. Nel *dark web* è possibile per i criminali informatici scambiarsi informazioni, cooperare tra di loro e condividere le loro conoscenze tecniche: vi sono molti video *tutorial*, anche gratuiti, nei quali viene spiegato come utilizzare efficacemente le carte di credito clonate, creare dei *malware*, riciclare *Bitcoin*, ecc.[186]. Infine, vi sono le piattaforme decentralizzate di commercio, nelle quali manca un centro di regolazione, che però non sembrano svolgere un ruolo rilevante nel commercio illegale di beni[187].

I criminali informatici sfruttano anche l'intelligenza artificiale (di seguito IA) per i loro scopi illeciti. L'IA può essere utilizzata per migliorare gli attacchi informatici, in particolare quelli commessi tramite la tecnica del *phishing*, poiché aiuta a creare finti messaggi che appaiono sempre più autentici, includendo informazioni reperite sui *social network* o simulando lo stile di scrittura di una persona fidata. L'IA consente di non inviare messaggi truffaldini uniformi a tutti gli obiettivi, ma di personalizzarli per ingannare un maggior numero di vittime[188]. È stato dimostrato che l'IA può essere utilizzata per commettere un attacco di *spoofing* contro i sistemi *Wi-Fi* ed intercettare così i dati sensibili degli utenti (quali codici fiscali, numeri di carte di credito, credenziali, ecc.), garantendo un livello di anonimato maggiore rispetto ad un attacco informatico perpetrato con modalità tradizionali[189]. L'IA può essere sfruttata per individuare le vulnerabilità di un particolare sistema informatico, favorendo la realizzazione di attacchi informatici massicci su larga scala, ma efficaci, e addirittura per sfuggire ai controlli da parte di altri sistemi di IA volti a prevenire gli attacchi informatici[190].

---

[185] *Ibid*., p. 53.
[186] VAN HARDEVELD G. J., WEBBER C., O'HARA K., *Discovering credit card fraud methods in online tutorials*, in *Proceedings of the Workshop on Online Safety, Trust and Fraud Prevention. ACM Web Science Conference*, New York, 2016, p. 1 ss., p. 1.
[187] WÜST M., *Die Underground Economy*, cit., p. 66.
[188] CADWELL M., ANDREWS J.T.A., TANAY T., GRIFFIN L.D., *AI-enabled future crime*, in *Crime Sci.*, 2020, vol. 9, n. 14, p. 1 ss., p. 8.
[189] PAGALLO U., QUATTROCOLO S., *The impact of AI on criminal law, and its twofold procedures*, in W. Bartfield, U. Pagallo, *Research handbook on the law of artificial intelligence*, Cheltenham, 2018, p. 385 ss., p. 400.
[190] AA.VV., *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*, *Report* disponibile *online* all'indirizzo https://arxiv.org/abs/1802.07228, p. 18. In informatica, infatti, vengono indicati come attacchi *zero-day* o *0-day* quegli sferrati dagli *hacker* sfruttando una falla di sicurezza del sistema di cui il fornitore e lo sviluppatore non erano neppure a conoscenza. Per approfondire v. ZHANG M., WANG L., JAJODIA S., SINGHAL A., *Network Attack Surface: Lifting the Concept of Attack Surface to the Network Level for Evaluating Networks' Resilience Against Zero-Day Attacks*, in *IEEE Trans. Dependable Secure Comput.*, 2021, vol 18, n.1, p. 310 ss., p. 310.

4.4. Le criptovalute come strumento o oggetto del reato.

L'utilizzo delle criptovalute consente di monetizzare i dati di carte di credito, *password*, ecc. illecitamente carpiti, cosa che in precedenza non era agevole, e rende i pagamenti nei riscatti a seguito di *ransomware* più facili e non tracciabili[191]. Come sopra evidenziato, il *Bitcoin* si presta efficacemente ad operare quale mezzo di scambio nel campo delle attività illegali e criminali, tant'è che è il mezzo di pagamento preferito nel *darkweb*[192].

Bitcoin e le criptovalute in generale si prestano poi bene anche a realizzare operazioni di riciclaggio di denaro[193], dato che consentono di realizzare transazioni elettroniche transfrontaliere in modo anonimo. Tant'è che si presume che nel solo anno 2018 ben 4,6 miliardi di euro siano stati riciclati in Europa esclusivamente attraverso le criptovalute[194]. Nella maggior parte dei casi i criminali non si limitano a trasferire il valore monetario all'interno di una *blockchain*, ma, come sopra esaminato, sfruttano anche i c.d. servizi *tumbler* o *mixer*, utilizzati per rendere praticamente impossibile la tracciabilità delle transazioni.

Sia nel riciclaggio di denaro, sia nell'acquisto di prodotti e servizi illeciti sul *dark web* le criptovalute sono utilizzate come un mero strumento. Vi sono però altri casi in cui la criptovaluta, e i *token* sopra descritti (v. *supra*, par. 2) costituiscono oggetto del reato[195]. Infatti, gli stessi *Bitcoin*, esattamente come la moneta elettronica, possono essere sottratti al titolare tramite attacco informatico diretto a sottrarre le chiavi crittografiche a protezione del *wallet*[196]. Il fatto che la maggior parte delle criptovalute non siano custodite in *wallet* privati, bensì in *online-wallet* gestiti da determinati gestori (v. *supra* par. 2), rende l'attacco in questione più agevole[197]. Questo perché l'*hacker* può colpire direttamente il sistema dell'*exchanger*, appropriandosi delle chiavi private dei *wallet* dei clienti da lui detenute e in questo modo appropriarsi delle criptovalute ivi custodite. A tal proposito, è stata segnalata l'esistenza di un *malware* denominato *Pony* specificamente progettato per sottrarre le

[191] LEWIS J., *Economic Impact of Cybercrime*, cit., p. 6.
[192] HÖNIG M., *ICO und Kryptowährungen*, cit., p. 80.
[193] PICOTTI L., *Profili penali del cyberlaundering: le nuove tecniche di riciclaggio*, in *Riv. trim. dir. pen. econ.*, 2018, n. 3- 4, p. 594 ss., p. 599; CROCE M., *Cyberlaundering e valute virtuali. La lotta al riciclaggio nell`era della distributed economy*, in *Sist. Pen.*, 2021, n. 4, p. 127 ss., p. 148; STURZO L., *Bitcoin e riciclaggio 2.0*, in *Dir. pen. cont.*, 2018, n. 5, p. 19 ss., p. 19.
[194] BELE J., *Cryptocurrencies as facilitators of cybercrime*, in *SHS Web Conf.*, 2021, vol. 111, p. 1 ss., p. 5.
[195] DAL CHECCO P. (a cura di), *Diritto penale e processuale*, in S. Capaccioli (a cura di), *Criptoattività, criptovalute e bitcoin*, Milano, 2021, p. 271 ss., p. 303.
[196] SIXT E., *Bitcoins und andere dezentrale Transaktionssysteme*, cit., p. 92.
[197] ROSEMBERGER P., *Bitcoin und Blockchain*, cit., p. 143.

criptovalute custodite nei *wallet* installati su *smartphone* o *computer*[198]. Inoltre, gli attacchi *hacker* possono essere diretti anche contro i *mining pool*, per cui il criminale informatico prende il controllo del sistema di creazione delle criptovalute e riesce a crearne direttamente in proprio favore. Non solo, ma attraverso l'utilizzo di codici *malware* può impossessarsi delle chiavi private dei *miners* o modificare gli indirizzi della *mining pool* in modo tale che le criptomonete di nuova creazione vengano direttamente dirottate nel suo *wallet*[199].

Oltre alle criptovalute, anche la stessa tecnologia *blockchain* può essere sfruttata per scopi criminali. Infatti, di recente sono stati sviluppati i c.d. *criminal smart contract*, nei quali la prestazione dedotta nel contratto corrisponde ad un'attività illecita, ovvero la rivelazione di informazioni segrete o chiavi private altrui oppure la commissione di reati nel mondo reale, come ad esempio un omicidio su commissione[200].

Gli attacchi informatici contro il patrimonio possono essere i più disparati e vanno dal posizionamento dello *skimmer* in un terminale per l'utilizzo di carte di credito agli attacchi volti a sovraccaricare il sito di un'infrastruttura dello Stato. Tutti, però, hanno lo stesso obiettivo in comune, ovvero alterare il normale funzionamento del sistema informatico[201]. Per stabilire la responsabilità penale degli autori di tali attacchi è indispensabile individuare il meccanismo da loro utilizzato. Pertanto, i prossimi paragrafi saranno dedicati all'analisi delle specifiche tecniche utilizzate dai criminali informatici per realizzare truffe e frodi *online*.

5. I diversi schemi di truffe *online*: *nigerian scams, charity* e *dating scams*.

Lo sviluppo del commercio *online* (o *e-commerce*)[202] ha comportato una notevole semplificazione e rapidità degli scambi economici, che ora possono avvenire in brevissimo

[198] CHOO K.R., *Cryptocurrency and Virtual currency: Corruption and Money Laundering/Terrorism Financing Risks?*, in D.L. Kuo Chuen, *Handbook of digital currency. Bitcoin, innovation, financial instruments, and big data*, Amsterdam, 2015, p. 283 ss., p. 300. A livello mondiale è famoso l'attacco di tipo *hacking* che ha colpito la società giapponese Mt. Gox, leader mondiale tra le società di *exchange*, alla quale nel febbraio del 2014 sono stati sottratti ben 850.000 Bitcoin, v. HÖNIG M., *ICO und Kryptowährungen*, cit., p. 19.

[199] DAL CHECCO P. (a cura di), *Diritto penale e processuale*, cit., p. 305.

[200] ACCINNI G., *L'utilizzo criminogeno della blockchain*, cit., p. 137.

[201] SHAMSI J.A., ZEADALLY S., SHEIKH F., FLOWERS A., *Attribution in cyberspace: techniques and legal implications*, in *Security Comm. Networks*, 2016, vol. 9, n. 15, p. 2886 ss., p. 2886.

[202] Da non confondere con il commercio elettronico, che la Commissione Europea nella Comunicazione n. 157 del 15 aprile 1997 definisce come «*lo svolgimento di attività commerciali per via elettronica. Basato sull'elaborazione e la trasmissione di dati (tra cui testo, suoni e immagini video) per via elettronica, esso comprende attività disparate quali: commercializzazione di merci e servizi per via elettronica; distribuzione on-line di contenuti digitali; effettuazione per via elettronica di operazioni quali trasferimenti di fondi, compravendita di azioni, emissione di polizze di carico, vendite all'asta, progettazione e ingegneria in cooperazione; on-line sourcing; appalti pubblici per via elettronica, vendita diretta al consumatore e servizi*

tempo e svolgersi interamente *online*. Esso ha, però, favorito nuove possibilità per i criminali di delinquere, i quali sfruttano il fatto che le trattative si svolgono solitamente senza le formalità che caratterizzano le contrattazioni tradizionali e, soprattutto, senza un controllo preventivo sull'identità dei contraenti e sulla rispondenza dei prodotti alle descrizioni. Gli schemi delle truffe tradizionali si sono progressivamente spostati sul *web* e, in alcuni casi, si sono evolute in modo significativo, come, ad esempio, i c.d. schemi Ponzi.

Le truffe su piattaforme di *e-commerce* rappresentano un'elevata quota del *cybercrime*. Tali truffe possono avvenire sia su siti *web* realmente esistenti dedicati alla vendita di beni o servizi (quali ad esempio *subito.it*, *ebay.it*, ecc.), sia su siti c.d. *fake*, appositamente creati per ingannare l'acquirente[203].

I criminali possono facilmente raggirare le vittime con profili falsi su piattaforme *online*, accompagnate da fotografie dei prodotti asseritamente in vendita appartenenti a terzi estranei e inconsapevoli oppure artefatte *ad hoc*. Queste tipologie di truffe possono essere articolate secondo modalità diverse per frodare sia il potenziale acquirente che il potenziale venditore. Nel primo caso il truffatore finge di mettere in vendita un bene al solo scopo di ottenere dal potenziale acquirente una somma di denaro attraverso bonifici o carte di credito, senza inviare alcun bene o inviando un prodotto non funzionante o non rispondente alle caratteristiche descritte e pattuite[204]. Nel secondo caso agli annunci *online* spesso risponde un presunto potenziale acquirente, che sostiene di voler pagare in anticipo, ma poco dopo l'invio della merce finge dei problemi col versamento e chiede al venditore di inviargli copia dei suoi documenti di identità (per compiere altre truffe utilizzando abusivamente l'identità della vittima come schermo) e/o somme di denaro[205]. In altri casi il truffatore invia al venditore un assegno (quasi sempre emesso da banche estere) apparentemente regolare, ma in realtà falsificato. Per ingannare la vittima, si indica spesso una filiale dismessa di un istituto bancario realmente esistente, ma che sui motori di ricerca risulta erroneamente ancora aperta[206]. In questi casi quando l'istituto di credito si accorge con giorni di ritardo che l'assegno è falsificato il bene è già stato inviato al truffatore. Questo metodo prevede

post-vendita». L'*e-commerce*, dunque, è una realtà più ristretta del commercio elettronico. Per approfondimenti v. CIPOLLA P., *E-commerce e truffa*, in *Giur. mer*., 2013, n. 12, p. 2624 ss., p. 2624.

[203] CAJANI F., CAVALLO F., *Le truffe su piattaforma di e-commerce: l'esperienza della procura di Milano*, in G. Costabile, A. Attanasio, M. Ianulardo (a cura di), *IISFA Memberbook 2015 – Digital Forensic*, Forlì, 2015, p. 19 ss., p. 19 s.

[204] *Ibid*., p. 20.

[205] *Ibid.*

[206] Per approfondimenti v. la videoinchiesta del noto programma televisivo Striscia la Notizia, disponibile al sito https://www.striscialanotizia.mediaset.it/video/compravendita-di-auto-la-truffa-degli-assegni-falsi-continua_77685.shtml

un'ulteriore variante, ovvero l'invio di assegno di falso, ma di importo superiore al prezzo pattuito, cui poco dopo, con la scusa dell'errore, farà seguito la richiesta del truffatore di restituzione di restituzione della somma eccedente via *Western Union*[207]. I nuovi metodi di pagamento e soprattutto i metodi di trasferimento di denaro (come *Western Union* o *Money Gram*), più aleatori rispetto a quelli tradizionali, hanno oggettivamente agevolato la realizzazione di questo tipo di truffe[208].

Molto frequenti sono le truffe relative all'affitto di appartamenti: anche in tale ipotesi il truffatore finge di avere la disponibilità di beni immobili, mettendo su appositi siti *web* finti annunci o rispondendo ad annunci di persone che cercano casa. Dopodiché il truffatore sostiene di trovarsi all'estero e di non poter mostrare l'appartamento, di cui spesso invia fotografie che, però, riguardano ignari proprietari, e sostiene di voler utilizzare *Airbnb*, noto portale per la prenotazione *online* di alloggi, per la gestione dell'appartamento. A quel punto chiedono alla vittima l'invio dei suoi documenti, che utilizzeranno poi come falsa identità per una successiva truffa, e creano un finto annuncio su un sito clone di quello di *Airbnb*, sul quale richiedono alla vittima di prenotare. Una volta fatto ciò, inseriscono i dati per un bonifico e chiedono alla vittima di versare una caparra, nonché il versamento dell'affitto[209].

La giurisprudenza si è mostrata consapevole della pericolosità di tali nuovi fenomeni criminosi, ritenendo applicabile la circostanza aggravante della minorata difesa in caso di cui al n. 5 dell'art. 61 c.p. nel caso in cui le trattative si siano svolte integralmente *online*[210], come si avrà modo di vedere in seguito (v. *supra*, cap. III, par. 1).

5.1. I c.d. schemi Ponzi.

Il *web* consente anche il proliferare di schemi fraudolenti conosciuti come schemi Ponzi[211], che oggi funzionano anche con le criptovalute. Essi non sono che schemi economici truffaldini nei quali il truffatore attira e recluta le vittime promettendo loro di investire il loro denaro in attività finanziarie o speculative dai rendimenti elevati e a basso rischio[212]. Tali attività finanziarie e speculative, in realtà, non esistono, ma il truffatore inizialmente paga i

[207] CAJANI F., CAVALLO F., *Le truffe su piattaforma di e-commerce*, cit., p. 20.
[208] *Ibid.*, p. 21.
[209] Cfr. https://quifinanza.it/info-utili/case-in-affitto-truffa-airbnb/336703/. Questo tipo di truffa non è molto analizzato, ma recentemente sono stati segnalati numerosi tentativi di truffa del genere.
[210] V., da ultimo, Cass. pen., sez. VI, 6 maggio 2022, n. 18252.
[211] La denominazione deriva dal nome di Charles Ponzi, l'inventore di questa tipologia di frode. Italiano emigrato negli Stati Uniti d'America, negli anni '20 del secolo scorso divenne noto per una truffa su larga scala perpetrata tramite i buoni postali di risposta internazionale. Per approfondire v. il romanzo di F. Mazzotti e P. Bernardelli, *Lo schema Ponzi. Romanzo di una truffa*, Milano, 2021.
[212] ZHU A., FU P., ZHANG Q., CHEN Z., *Ponzi scheme diffusion in complex networks*, in *Physica A*, 2017, vol. 479, p. 128 ss., p. 128.

primi rendimenti o tassi di interesse ai primi investitori utilizzando i soldi dei nuovi sottoscrittori, in modo tale da convincere le vittime che si tratti di un affare redditizio. In questo modo si sparge la voce che si tratta effettivamente di un investimento vantaggioso ed è più facile per il truffatore reclutare nuove vittime. Tale truffa può terminare in due modi: nel primo caso il truffatore, una volta raggiunto il massimo profitto, sparisce trattenendo il denaro ricevuto, nel secondo caso il sistema collassa per difficoltà di reperire nuove vittime ed il truffatore fa perdere le sue tracce trattenendo il denaro ricevuto[213]. Gli schemi Ponzi si accompagnano spesso ai c.d. schemi piramidali, nei quali il truffatore spinge le vittime a reclutare nuove vittime, promettendo loro rendimenti più elevati e questo garantisce un afflusso continuo di partecipanti[214].

Questo schema truffaldino è tornato di recente *in auge* ed è approdato sul *web* con il nome di *High Yield Investment Program*, perché i siti che lo promuovono promettono altissimi tassi d'interesse a fronte di pochissimi rischi[215]. A sostegno del c.d. HYIP si è sviluppato un vasto ecosistema *online*, che comprende siti *web* di discussione, valute virtuali e siti web "aggregatori" di terze parti, che tengono traccia delle prestazioni delle HYIP. In questi ultimi siti i primi investitori individuano le nuove vittime[216]. Non è raro che svariati *influencer*[217], più o meno in buona fede, sponsorizzino i c.d. HYIP, invitando le persone ad investire i loro risparmi in tali attività truffaldine.

Anche in questo caso le criptovalute svolgono un ruolo fondamentale: nella maggior parte dei casi i truffatori richiedono che l'investimento iniziale venga fatto in criptovalute, perché questo tipo di transazioni non consentono di risalire alle rispettive identità e non sono revocabili da parte delle vittime[218]. Nei nuovi schemi Ponzi le criptovalute non sono solo uno strumento di pagamento. In molti casi, infatti, lo schema truffaldino riguarda proprio le criptovalute e gli *smart contract* ad esse correlati (v. *supra* par. 3). Nel primo caso, i truffatori convincono le vittime ad investire in nuove criptovalute, promettendo in cambio il

[213] AMOAH B., *Mr Ponzi with Fraud Scheme Is Knocking: Investors Who May Open*, in *Glob. Bus. Rev*., 2018, vol. 19, n. 5, p. 1115 ss., p. 1117.
[214] *Ibid*.
[215] MOORE T., HAN J., CLAYTON R., *The Postmodern Ponzi Scheme: Empirical Analysis of High-Yield Investment Programs*, in A.D. Keromytis (eds.), *Financial Cryptography and Data Security. FC 2012. Lecture Notes in Computer Science*, Heidelberg, 2012, p. 41 ss., p. 41.
[216] *Ibid*., p. 42.
[217] Definito come «*personaggio di successo, popolare nei social network e in generale molto seguìto dai media, che è in grado di influire sui comportamenti e sulle scelte di un determinato pubblico*», in Enc. Treccani online, disponibile all'indirizzo https://www.treccani.it/vocabolario/influencer_res-728101ee-89c5-11e8-a7cb-00271042e8d9_%28Neologismi%29/
[218] MOORE T., HAN J., CLAYTON R., *The Postmodern Ponzi Scheme*, cit., p. 49.

pagamento di commissioni o rendimenti elevatissimi[219]. Nel secondo caso, gli schemi Ponzi sono presenti su *smart contract* di *blockchain* realmente esistenti e funzionanti, quale, ad esempio, *Bitcoin* o *Ethereum*[220].

La diffusione degli schemi Ponzi, sotto forma di *smart contract*, è agevolata dal fatto che il truffatore ha la possibilità di rimanere anonimo e che il contratto truffaldino, in assenza di un'autorità centrale che controlli, non può essere dichiarato nullo o risolto; lo schema fraudolento non può essere interrotto prima del tempo stabilito dal truffatore[221]. Per questo motivo, vi è chi ritiene che gli *smart contract* abbiano mutato la modalità di esecuzione degli schemi Ponzi. Se in precedenza potevano essere interrotti in qualsiasi momento, in questo caso è necessario attendere che le condizioni previste nel codice dello *smart contract* siano state tutte soddisfatte[222]. L'immutabilità del suddetto codice consente al truffatore di ingannare le sue vittime. Il fatto che il codice dello *smart contract* sia pubblico ed immutabile le porta a credere che il proprietario dello stesso non si possa approfittare di loro, che lo schema sia destinato a durare per sempre e di avere una buona probabilità di ottenere gli interessi dichiarati[223]. In questo caso i truffatori creano uno *smart contract* che prevede la distribuzione di denaro agli investitori, che sono gli utenti che hanno inviato del denaro per la sua creazione. Il denaro che serve a ripagare gli investitori proviene esclusivamente da detto contratto, dunque si basa sulle nuove sottoscrizioni. L'utente, dunque, può realizzare un profitto solo se attrae nuovi investitori, *alias* vittime della truffa. Una volta che non vi

[219] DAL CHECCO P. (a cura di), *Diritto penale e processuale*, cit., p. 304. Celebre, a livello mondiale, è la truffa OneCoin. La cittadina bulgara Ruja Ignatova e i suoi complici promettevano alle vittime che la loro criptovaluta avrebbe in breve tempo soppiantato il Bitcoin, per cui avrebbero ricavato profitti straordinari in poco tempo, oltre che bonus aggiuntivi qualora gli aderenti all'investimento avessero reclutato ulteriori soci-investitori. Alle vittime veniva fatto credere non solo che al crescere del numero degli investitori sarebbe aumentato significativamente il valore della criptovaluta sul mercato, ma anche che era possibile la conversione in valuta corrente, attraverso una non meglio precisata quotazione in borsa della moneta. Una volta raggiunto un numero considerevole di investitori, i truffatori sono scomparsi trattenendo con sé i risparmi delle vittime. L'ammontare dei fondi sottratti fraudolentemente ad investitori in tutto il mondo è di circa 4 miliardi di euro. V. https://www.ildolomiti.it/cronaca/2021/promettevano-guadagni-straordinari-con-la-criptovaluta-onecoin-ma-era-una-truffa-quasi-4mila-gli-altoatesini-che-hanno-acquistato-i-pacchetti

[220] VASEK M., MOORE T., *Analyzing the Bitcoin Ponzi Scheme Ecosystem*, in AA. VV., *Financial Cryptography and Data Security. FC 2018. Lecture Notes in Computer Science*, Heidelberg, 2019, p. 101 ss., p. 101.

[221] BARTOLETTI M., CARTA S., CIMOLI T., SAIA R., *Dissecting Ponzi schemes on Ethereum: identification, analysis, and impact*, in *Future Gener. Comput. Syst*., 2020, Vol. 102, p. 259 ss., p. 260.

[222] AA. VV., *Detecting Ethereum Ponzi Schemes Based on Improved LightGBM Algorithm*, in *IEEE Trans. Inf. Forensics Secur*., 2022, vol. 9, n. 2, p. 624 ss., p. 624, in cui si evidenzia come «*The Ethereum smart contract endows the Ponzi scheme with new characteristics. Traditional Ponzi schemes can be terminated artificially, and their organizer can disappear with the money at any time. In the Ethereum smart contract, a Ponzi scheme can be written into the code of the smart contract and cannot be terminated artificially. The Ponzi scheme cannot be terminated automatically unless conditions preset in the smart contract code are satisfied*».

[223] BARTOLETTI M., CARTA S., CIMOLI T., SAIA R., *Dissecting Ponzi schemes on Ethereum*, cit., p. 260.

sono più nuovi investitori disposti ad investire nel contratto, lo *smart contract* termina e le vittime perdono per sempre il capitale investito[224].

5.2. Le *advance fee fraud*.

Un'altra tipologia di truffa particolarmente diffusa sul *web* è costituita dalle c.d. *advance fee fraud* (AFF) o frode delle commissioni anticipate. Secondo tale schema il truffatore convince le sue vittime a pagare una somma di denaro a titolo di anticipo per il pagamento di una tassa, di una tangente, ecc., promettendogli in cambio una maggior somma di denaro a titolo di remunerazione[225]. In questa tipologia di schema truffaldino rientrano le c.d. truffe alla nigeriana o *nigerian scams*, dette anche *419 scams* dal numero del codice penale nigeriano che punisce il reato di truffa. Questa tipologia di frode in origine prevedeva l'invio di una *mail* ad una serie di destinatari nella quale il mittente fingeva di essere un funzionario del governo nigeriano oppure un principe nigeriano in possesso di una grossa somma di denaro e necessitante di aiuto dall'estero per trasferirla fuori dalla Nigeria prima della sua imminente confisca da parte del governo.

Nella quasi totalità dei casi il patrimonio asseritamente posseduto ammonta a svariati milioni di dollari, in modo da rendere l'offerta più allettante e far leva sull'avidità della vittima[226]. In cambio di tale aiuto, che si sostanziava nella messa a disposizione del proprio conto corrente, il mittente prometteva una percentuale variabile della somma da lui asseritamente detenuta (in genere del venti o trenta percento). A quel punto cominciavano le conversazioni via *mail* tra l'asserito funzionario e la vittima, per accordarsi sul trasferimento della somma di denaro. Prima che la somma potesse essere accreditata sul conto corrente della vittima l'asserito funzionario prospettava alla vittima la necessità di pagare una serie di somme a titolo di commissioni bancarie, (tangenti per la corruzione, tasse, ecc.) sostenendo di non poter procedere alla spesa per via di problemi burocratici. Una volta incassata tale somma, il criminale scompariva senza più lasciare traccia[227]. Questo tipo di truffa oggi ha assunto portata internazionale ed è diventato molto più sofisticato. Mentre in origine il testo del linguaggio dei messaggi era generico e poco preciso, l'evoluzione tecnologica ha ridotto questo problema e spesso nel testo delle *mail* è riportato il nome del destinatario. Le vittime vengono accuratamente scelte tramite *social network* e i truffatori

[224] *Ibid.*, p. 264 s.
[225] RICH T., *You can trust me: a multimethod analysis of the Nigerian email scam*, in *Secur J*, 2018, n. 31, p. 208 ss., p. 208.
[226] *Ibid*., p. 214.
[227] RIBIC P., *The Nigerian email scam novel*, in *J. Postcolon. Writ.*, 2020, vol. 55, n. 3, p. 424 ss., p. 425.

prima sviluppano un rapporto di amicizia virtuale con la vittima per indurla a fidarsi di loro e solo dopo un certo lasso di tempo le chiedono aiuto per il finto trasferimento di una grossa somma di denaro[228]. Oggi non si fa più riferimento esclusivo alla Nigeria. Nella maggior parte dei casi il truffatore utilizza una rete *Virtual Private Network* e fingere di trovarsi o risiedere nello stesso Paese della vittima, in modo da conquistarne più facilmente la fiducia[229].

Questa tipologia di truffa può avere epiloghi drammatici. A tal proposito, è sufficiente ricordare che nel 2003 il diplomatico nigeriano Michael Lekara Wayid, in servizio in Repubblica ceca, fu ucciso a colpi di fucile da un ultrasettantenne, convinto di attuare una vendetta contro colui che lo aveva raggirato con questo sistema[230].

Di tale tipologia di truffa esistono diverse varianti. La più nota prende il nome di *spanish prisoner* (o prigioniero spagnolo), risalente addirittura al sedicesimo secolo, nella quale il truffatore finge di essere amico di un nobile spagnolo, detenuto per motivi politici e che non può rivelare la sua identità per timore di ripercussioni. Tale prigioniero è asseritamente titolare di un ingente patrimonio e sta cercando una persona onesta che lo possa amministrare, ovvero la vittima, in attesa del suo rilascio, la quale, in cambio di tale aiuto, sarà generosamente ricompensata. Il truffatore chiede pertanto alla vittima contattata *online* di anticipare una somma di denaro che dovrà servire per il rilascio del prigioniero[231]. Anche questo tipo di truffa viene oggi perpetrata attraverso *social network*.

Altra variante è quella della finta lotteria, ove i truffatori inviano una *mail*, che annuncia la vincita di una somma ingente ad una lotteria poco conosciuta, di solito in un paese straniero. Dopo il primo contatto, i truffatori chiedono alla vittima di pagare una piccola somma per "rilasciare" le vincite, da versare su un conto personale estero. In questo caso i truffatori non necessariamente inviano delle *mail*, ma possono utilizzare anche i *banner* di un sito o, più comunemente, un sito *pop up*[232].

Altre ancora sono le c.d. *charity scams*, nelle quali i truffatori chiedono soldi alle vittime fingendo siano destinati a falsi progetti di beneficienza. In molti casi i truffatori approfittano di tragedie o catastrofi, nonché della generosità delle persone, e a tal fine

---

[228] BORDY R., KERN S., OGUNADE K., *An insider's look at the rise of Nigerian 419 scams*, in *J. Financ. Crime*, 2022, vol. 29, n. 1, p. 202 ss., p. 204.
[229] *Ibid*., p. 209.
[230] https://www.telegraph.co.uk/finance/2846265/Parting-a-fool-and-his-money.html
[231] GILLESPIE A.A., *The Electronic Spanish Prisoner: Romance Frauds on the Internet*, in *J. Crim. L.*, 2017, vol. 81, no. 3, p. 217 ss., p. 218.
[232] WHITTY M.T., *Is There a Scam for Everyone? Psychologically Profiling Cyberscam Victims*, in *Eur. J. Crim. Policy Res.*, 2020, n. 26, p. 399 ss., p. 400.

utilizzano i *social network* quali *Facebook*, *YouTube* o *Instagram* nonché siti di raccolta di risparmio o *crowdfunding* per raccogliere le donazioni[233].

Infine, vi sono le c.d. *employment scams* o truffe occupazionali, nelle quali i truffatori inseriscono su portali *online* finte offerte di lavoro e poi chiedono alle vittime di pagare una somma di denaro a vario titolo (tasse, IVA, ecc.) per poter stipulare il contratto[234].

L'*Online dating scam* (o truffa sentimentale) è particolarmente insidiosa perché crea danni psicologici anche a lungo termine nelle vittime[235]. In questo caso i truffatori sfruttano i sentimenti della vittima e fanno leva sul suo bisogno di affetto e sul suo senso di empatia. Nonostante questa truffa sia ormai comunemente nota, le vittime sono ancora moltissime e le perdite finanziarie ad esse recate notevoli[236].

I criminali informatici creano finti profili su siti di incontri *online*, nonché sui *social network* o siti di messaggistica quali *whatsapp*, accompagnati da una falsa foto e/o di un profilo di persone realmente esistenti, ma ignare, o totalmente artefatta per ingannare la vittima. L'immagine viene scelta in modo da essere più attraente possibile. Spesso utilizzano un finto numero telefonico per non far conoscere la loro reale ubicazione[237]. A quel punto contattano la vittima prescelta, mandandole una richiesta di "amicizia" o di poter diventare un suo *follower*. Il truffatore comincia, quindi, a contattare la vittima, rivelandole finti dettagli intimi e dolorosi della propria vita privata, in modo da carpirne la fiducia. A sua volta la vittima si confida con il truffatore. A quel punto cominciano le richieste di denaro, giustificate da motivi più disparati, quali una malattia improvvisa o un incidente, il furto di documenti, problemi familiari oppure anche soldi per i biglietti per il viaggio per incontrare la stessa vittima[238]. Le richieste di denaro si fanno sempre più pressanti e, in caso di rifiuto, la vittima viene ricattata. Altre volte i truffatori promettono di restituire il denaro alle vittime il prima possibile. In altri casi chiedono e ottengono dalla vittima l'invio di contenuti

---

[233] *Ibid*.
[234] *Ibid*.
[235] KOPP C., LAYTON R., SILLITOE J., GONDAL I., *The Role of Love stories in Romance Scams: A Qualitative Analysis of Fraudulent Profiles*, in *Int. J. Cyber Criminol*., 2015, vol. 9, n. 2, p. 205 ss., p. 206; REGE A., *What's Love Got to Do with It? Exploring Online Dating Scams and Identity Fraud*, in *Int. J. Cyber Criminol*., 2009, vol. 3, n. 2, p. 494 ss., p. 497.
[236] L'FBI ha riportato che nel solo 2021 circa 24.000 vittime negli Stati Uniti d'America hanno dichiarato di aver perso circa 1 miliardo di dollari a causa di truffe sentimentali. In argomento v. il sito dell'FBI all'indirizzo https://www.fbi.gov/contact-us/field-offices/houston/news/press-releases/1-billion-in-losses-reported-by-victims-of-romance-scams.
[237] BORDY R., KERN S., OGUNADE K., *An insider's look*, cit., p. 210.
[238] REGE A., *What's Love*, cit., p. 498.

pornografici, che poi useranno per ricattarla e convincerla a continuare con l'invio di somme di denaro e come deterrente per fare in modo che non si rivolgano alle forze dell'ordine[239].

Dietro queste tipologie di truffe operano in molti casi associazioni a delinquere a struttura flessibile, nelle quali i membri vengono reclutati a seconda delle necessità. In questo ambito, si distinguono gli organizzatori, *extenders*, ovvero coloro che si occupano di espandere la rete criminale, gli esecutori, che per questo genere di truffe devono possedere notevoli doti persuasive e, infine, gli *enforcers*, ovvero coloro che si occupano di tutelare i criminali minacciando le vittime per dissuaderle dal presentare denuncia[240].

Il problema maggiore per questo tipo di truffe è che i sistemi tradizionali per individuare i falsi profili utilizzati dai siti di incontri *online* sono in larga parte inefficaci, perché si basano su un sistema di liste nere di indirizzi IP o *proxy* per identificare i presunti truffatori, ovvero lo stesso utilizzato per il filtraggio delle *mail* di *spam*. Ma tali truffe non vengono eseguite con campagne su larga scala, né i profili sono generati automaticamente, dato che i messaggi inviati alle vittime sono personalizzati. Per questo motivo, aggirare tali sistemi di controllo è estremamente agevole[241]. Tuttavia, negli ultimi tempi è stato elaborato un sistema piuttosto efficace, che però funziona unicamente per i siti di incontri, che consente di individuare i falsi profili sulla base dell'immagine del profilo e del linguaggio utilizzato[242].

6. *Phishing*, *Vishing*, *Pharming*, *Sim fraud swapping*, *Carding*, *identity theft*: l'evoluzione delle tecniche di *social engineering* finalizzate al fraudolento conseguimento di un ingiusto profitto.

6.1. Il *phishing* e le sue varianti.

Oltre ad esportare le tradizionali modalità di truffa sul *web*, nel corso degli anni i criminali informatici hanno inventato, sperimentato e perfezionato nuove tecniche per derubare le vittime sfruttando le nuove tecnologie informatiche e il sempre più diffuso utilizzo dei nuovi strumenti di pagamento (v. *infra*, par. 3).

Le tecniche utilizzate dai criminali informatici sono le più disparate e spesso sconosciute. La più nota tecnica è sicuramente il *phishing*, che consiste in una tecnica di

[239] AA.VV., *Online Romance Scams: Relational Dynamics and Psychological Characteristics of the Victims and Scammers. A Scoping Review*, in *Clin. Pract. Epidemiol. Ment. Health*., 2020, n. 16, p. 24 ss., p. 25.
[240] REGE A., *What's Love*, cit., p. 502.
[241] AA. VV., *Automatically Dismantling Online Dating Fraud*, in *IEEE Trans. Inf. Forensics Secur*., 2020, vo. 15, p. 1128 ss., p. 1128.
[242] *Ibid.*, p. 1129 ss.

social engineering (o ingegneria sociale), volta a studiare il comportamento di un soggetto allo scopo di carpirne informazioni[243].

Il *phishing* classico, (o *deceptive phishing*), consiste nell'invio di *e-mail* abilmente contraffatte per indurre l'utente a fornire volontariamente le proprie informazioni personali[244]. Il *phisher* invia ad un elevato numero di destinatari dei messaggi contraffatti, che riportano nomi e loghi di istituti di credito o altre istituzioni "ufficiali", dal contenuto volto ad invitare colui che li riceve a cliccare su un apposito *link* ove vengono richiesti i codici identificativi dell'ente di riferimento, ad esempio *password* o *user ID*. Spesso si segnalano all'utente inesistenti problemi al *Server* dell'istituto bancario o la necessità (fittizia) di aggiornare i propri dati. Tale procedura secondo il finto messaggio dev'essere compiuta entro breve tempo cliccando sul *link* ivi contenuto[245].

Tale tecnica risale agli anni '90 del secolo scorso, ma è ancora oggi la forma più comune di *phishing*[246]. Sebbene la tecnologia dei sistemi antivirus per identificare siti e allegati portatori di *malware* si sia evoluta nel corso degli anni, non esiste ancora un sistema perfettamente funzionante in grado di identificare e censurare preventivamente tutte le *e-mail* di *phishing*, classificandole come dannose[247]. In origine, i finti messaggi erano rozzi e spesso contenenti errori di grammatica. Oggi, invece, sono molto più sofisticati: il *design* delle finte *mail* è molto ben curato, con loghi identici a quelli di società o istituzioni reali[248] e, soprattutto, sono personalizzate. Approfittando delle informazioni contenute *online* e sui *social network*, i criminali informatici possono selezionare più facilmente le loro potenziali vittime e inviare loro finti messaggi apparentemente riconducibili a collaboratori, fornitori, clienti e altre fonti affidabili[249]. Grazie allo *spoofing*, i criminali informatici possono inoltre

---

[243] CHANDLER D., MUNDAY R., voce *Phishing,* in *A Dictionary of Social Media*, 2016, Oxford; CAJANI F., COSTABILE G., MAZZARACO G., *Phishing e furto d'identità digitale*, *cit*., p. 12.

[244] FLOR R., *Phishing, identity theft e identity abuse. Le prospettive applicative del diritto penale vigente***,** in *Riv. it. dir. proc. pen.*, 2007, n. 2-3, p. 899 ss**.**, p. 900.

[245] Così CAJANI F., COSTABILE G., MAZZARACO G., *Phishing,* op. cit., p. 14.

[246] GHAZI-TEHRANI A., PONTELL H., *Phishing Evolves: Analyzing the Enduring Cybercrime*, in *Vict. Offenders*, 2021, vol. 16, n. 3, p. 316 ss., p. 319.

[247] RUTHERFORD R., *The changing face of phishing*, in *Comput. Fraud secur.*, 2018, n. 11, p. 6 ss. Anche se ad oggi non esiste una tecnica standard in grado di bloccare gli attacchi di *phishing*, tuttavia sono stati sviluppati, e si stanno sviluppando, diversi algoritmi per identificare e bloccare le *e-mail* di *phishing* prima che arrivino al mittente basate sul *machine learning*, sia *supervised* che *unsupervised*, per approfondire v. SAHINGOZ O. K., BUBER E., ONDER D., BANU D., *Machine learning based phishing detection from URLs*, in *Expert Syst. Appl.*, 2019, Vol. 117, n. 3, p. 345 ss.; ALMOMANI A., GUPTA B.B., ATAWNEH A., MEULENBERG A. e ALMOMANI E., *A Survey of Phishing Email Filtering Techniques*, in *Comm. Surv. Tutor.*, 2013, Vol. 15, n. 4, p. 2070 ss.

[248] Organization for Economic Co-operation and Development, *Scoping Paper on Online Identity Theft*, Seul, 2008, disponibile *online* al sito www.oecd.org/dataoecd/35/24/40644196.pdf p.16; VAYANSKY I., KUMAR S., *Phishing – challenges and solutions*, in *Comput. Fraud secur.*, 2018, n. 1, p. 15 ss.

[249] BODDY M., *Phishing 2.0: the new evolution in cybercrime*, in *Comput. Fraud Secur.*, 2018, n. 11, p. 8 ss., p. 9.

mascherare il reale indirizzo di provenienza delle *mail* di *phishing*, facendolo apparire come proveniente da un indirizzo *mail* affidabile[250].

Nell'anno 2022 ha preso piede una nuova campagna di *phishing* perpetrata attraverso false *mail* e messaggi *social*, che riportano il logo della Polizia di Stato e, in alcuni casi, sono artatamente firmate da dirigenti di vertice della Polizia[251]: in tali *mail* i truffatori sostengono che la vittima sarebbe indagata per gravi reati ("*pedopornografia, pedofilia, cyber pornografia, traffico sessuale*") e le intimano di rispondere alla *mail* per avere informazioni in merito all'indagine, minacciandola che altrimenti sarà arrestata. Lo scopo è di spaventare la vittima e indurla a ricontattare i mittenti del messaggio per fornire loro i propri dati personali.

Le variazioni rispetto al *deceptive phishing* sono moltissime, a cominciare dal *phishing* basato su *malware*[252]. Il *malware* può essere contenuto in un *software* che l'utente scarica da *Internet.* Paradigmatici sono gli *spyware* (quali il *keylogger* o lo *screenlogger*), che consistono in strumenti volti ad intercettare quanto viene digitato sulla tastiera o appare sullo schermo della vittima, oppure il *web Trojan*, vale a dire un programma che si aggancia ai sistemi di *login* per prelevare le credenziali della vittima[253].

Nel *phishing "man-in-the-middle",* vi è una combinazione tra attacco diretto e indiretto: il *phisher* intercetta i messaggi indirizzati ad un sito scelto da un qualsiasi utilizzatore, salva le informazioni che gli interessano, poi ritrasmette i messaggi al sito scelto dalla vittima ed infine le inoltra le risposte di ritorno[254].

Lo *Smishing* e il *vishing* sono varianti di *phishing* commessi tramite SMS o mediante telefono: l'utente viene convinto tramite SMS[255] o mediante *e-mail* a contattare il numero ivi fornito del proprio istituto bancario o altra istituzione, ovviamente fasullo, al quale risponde un finto operatore di *call center* o un nastro registrato, che invita l'utente a fornire le proprie generalità e i dati personali di identificazione[256], oppure a fornire le proprie credenziali di

---

[250] RAMESH BABU P., LALITHA BHASKARI D., SATYANARAYANA CH., *A Comprehensive Analysis of Spoofing*, in *JACSA*, 2010, vol. 1, n. 6, p. 157 ss., p. 158.

[251] https://www.poliziadistato.it/articolo/truffe-online-falsa-mail-della-polizia-di-stato

[252] Quest'ultimo termine viene solitamente impiegato per indicare un software che contiene un codice "maligno", la cui funzione consiste nel danneggiare o alterare dati informatici o un sistema informatico, per farne un uso diverso da quello previsto dai propri utenti. V. OECD, *Scoping Paper on Online Identity Theft*, cit., p. 16.

[253] Schematizzazione contenuta in CAJANI F., COSTABILE G., MAZZARACO G., *Phishing e furto d'identità digitale, op.cit.*, p. 28 s.

[254] *Ibidem*.

[255] Come avvenuto in un caso esaminato davanti all' ufficio del G.I.P. Di Milano, Trib. Milano, Ufficio G.I.P., 7 novembre 2007 in *Dir. Internet n.*3/2008, p. 261.

[256] PERRI P., *Lo smishing e il vishing, ovvero quando l'unico limite all'utilizzo criminale delle nuove tecnologie è la fantasia,* in *Dir. Internet,* n. 3, 2008, p. 261 ss., p. 266.

autenticazione al sistema bancario al finto *link* contenuto nell'SMS. Tramite la tecnica dello *spoofing*, è possibile occultare il numero telefonico reale e far apparire come mittente il vero numero telefonico dell'istituto bancario.

Lo *smishing* si è particolarmente diffuso a seguito del massiccio utilizzo da parte degli utenti delle *App* per usufruire dei servizi di *home banking*. A seguito dell'entrata in vigore del Regolamento delegato 2018/389/UE del 27 novembre 2017 della Commissione europea sulle norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri, di integrazione della direttiva 2015/2366/UE sui servizi di pagamento c.d. PSD2[257], la quasi totalità delle banche ha sostituito i vecchi *token* fisici necessari per l'autorizzazione delle operazioni *online* con apposite *App* per *smartphone*, che fungono da c.d. *token* virtuali. Se, da un lato, tale innovativo strumento è in grado di generare un nuovo codice usa e getta, collegato a una singola e unica operazione di pagamento, che avviene nei confronti di un unico beneficiario (a differenza dei vecchi dispositivi *token* che non erano in grado di fare), i nuovi *token* virtuali sono più vulnerabili. Per i criminali informatici è sufficiente che la vittima clicchi sul *link* contenuto nell'SMS truffaldino per avere la completa disponibilità del suo *token* virtuale, così da poterlo utilizzare per effettuare operazioni di pagamento a sua insaputa.

Per quanto riguarda il *vishing*, invece, il destinatario del messaggio truffaldino viene invitato ad effettuare una chiamata ad un finto *call center*, apparentemente riconducibile ad un'istituzione reale e a fornire le sue credenziali al finto operatore. Anche tale tipologia di *phishing* è tornata in auge: tramite apposita *App* i criminali informatici possono mascherare il loro numero telefonico e utilizzare un numero fittizio identico a quello dell'istituto di credito o altra entità (istituzione, istituto di credito, ecc.). Non solo, ma possono pure ingannare le vittime utilizzando appositi programmi per distorcere la loro voce e non essere così riconosciuti.

Il *pharming* è un'evoluzione del *phishing*[258]. La vittima viene ingannata per indurla a fornire le proprie credenziali e generalità, ma con una diversa e più sofisticata tecnica,

[257] La direttiva in questione, che in Italia è stata attuata dal d.lgs. 15 dicembre 2017 n. 218, prevede infatti all'art. 97 che il prestatore di servizi di pagamento "*applichi l'autenticazione forte"* quando il pagatore accede al suo conto di pagamento on line, dispone un'operazione di pagamento elettronico o effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi. L'autenticazione forte è definita dall'art. 4, co. 30, della direttiva come «*un'autenticazione basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente), che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione*».

[258] CAJANI F., COSTABILE G., MAZZARACO G., *Phishing*, cit., p. 37.

ovvero quella del sito "clone". In questo caso, la vittima viene reindirizzata su un sito "clone" dell'istituto di credito o dell'istituzione ed attraverso il *login* al falso portale vengono intercettate le sue credenziali. La navigazione sul sito *fake* avviene attraverso l'inserimento nel *computer* di un *malware* che modifica la lista dei siti contrassegnati come preferiti nel *browser* utilizzato dalla vittima[259].

Lo *spamming* consiste nell'invio di pubblicità indesiderate all'utente, per indurlo a cliccare su un *link* appositamente creato, contenente un *malware*[260]. A volte il *software* malevolo viene inviato con l'indicazione di avere come scopo la cancellazione dell'utente da una *mailing list* indesiderata. Gli schemi fraudolenti menzionati possono anche essere variamente combinati tra di loro. Basti pensare ad una possibile integrazione tra attacco basato su *malware*, che opera come *man-in-the-middle*.

Il fulcro offensivo del *phishing* e delle sue varianti, quindi, consiste sostanzialmente nel "furto di dati" riservati dall'utente al fine di farne un successivo uso non autorizzato[261]. Alla sottrazione *online* e all'utilizzo delle credenziali di accesso al sistema bancario o di altre istituzioni consegue, di regola, la realizzazione dell'evento materiale tipico, ovvero la diminuzione patrimoniale ai danni della vittima, conseguenza causale della. Coloro che si impossessano delle credenziali o dei dati personali altrui non sempre li utilizzano per commettere reati contro il patrimonio, ma possono anche, come si è visto in precedenza (v. *supra*, par. 4.2 e 4.3), venderli sul *dark web*, ove esiste un "mercato nero di identità" nel quale i dati delle vittime vengono spesso venduti da associazioni a delinquere operanti su scala globale[262].

Il fenomeno criminoso del *phishing* ha ormai assunto portata internazionale, mutando il profilo del *phisher*: non è più un mero *hacker*, o comunque soggetto con media o elevata competenza informatica, bensì un componente di gruppi criminali[263]. Nell'ambito del *Cybercrime-as-a-service* si sta affermando il *phishing-as-a-service*: i criminali informatici meno esperti possono acquistare appositi *kit* di pacchetti precostituiti, programmati in modo

[259] OECD, *Scoping Paper on Online Identity Theft, op. cit*., p. 19.
[260] *Ibid*., p. 20.
[261] FLOR R., *Phishing e profili penali dell'attività illecita di "intermediazione" del cd. financial manager*, in *Dir. pen. proc.*, n. 1, 2012, p. 55 ss., p. 56.
[262] Come rilevato dall'Organizzazione per la cooperazione e lo sviluppo economico in OECD, *Scoping Paper on Online Identity Theft,* op. cit., p. 22.
[263] Vi sono organizzazioni criminali appositamente dedite a creare ed inviare *e-mail* di *phishing*. In argomento v. Cajani, Costabile e Mazzarco in CAJANI F., COSTABILE G., MAZZARACO G., *Phishing,* cit., p.188., CLUSIT – Associazione italiana per la sicurezza informatica, *Rapporto 2019 sulla Sicurezza ICT in Italia*, Milano, 2019, consultabile al sito www. clusit.it/pubblicazioni/, che riporta un prezzo medio di 1.200 $ per l'acquisto di dati illecitamente sottratti di un utente medio.

da consentire all'acquirente di effettuare l'attacco in autonomia[264]. In tale contesto, è riduttivo equiparare il *phishing* ad una mera apprensione illecita dei dati altrui, dovendosi necessariamente considerare tutte le diverse fasi in cui esso si articola, nonché le conseguenze che da esso derivano.

Alcuni studi suddividono l'attività del *phishing* in tre fasi[265]. La prima riguarda l'ottenimento delle informazioni personali (tramite l'invio *dell'e-mail* di *phishing* o l'installazione del *malware*, ecc.); la seconda fase è caratterizzata dall'interazione con le credenziali o le informazioni personali illecitamente ottenute prima del loro utilizzo (ad es. il possesso o la vendita di tali dati); la terza, e ultima, fase consiste nell'utilizzo delle informazioni personali illecitamente ottenute per commettere altri reati (accessi abusivi, frodi, truffe, ecc.). Altri studiosi aggiungono un'ulteriore quarta fase, c.d. preparatoria, volta alla creazione ed al successivo invio delle *mail* di *phishing* o nella predisposizione di siti contraffatti[266].

6.2. Lo *sim swapping*, il *carding* e il furto d'identità digitale.

Tecnica altrettanto sofisticata è, oltre al *phishing*, lo *sim swapping*. In questo caso i criminali informatici, ingannando l'operatore telefonico, corrompendo i dipendenti del servizio clienti o sfruttando un *malware* che prende di mira la tecnologia *remote desktop* utilizzata nei *call center*[267], riescono ad ottenere illecitamente una scheda SIM clonata, tramite la quale procedono ad intercettare il codice aggiuntivo inviato tramite SMS per l'autenticazione e ad impossessarsi dell'*account* della vittima, modificandone le credenziali[268]. Notevole rilevanza hanno oggi gli attacchi informatici posti in essere mediante *malware*. Esistono tantissime tipologie di *malware*. I più diffusi sono i *Trojan Horse*, che consentono di accedere illegittimamente ai dati contenuti nel *computer* o nello *smartphone* altrui. Si celano, di regola, dietro *software* utili, così da indurre l'ignaro utente a scaricarli. Vi sono poi i *ransomware*, che impediscono all'utente di accedere a determinate

[264] GHAZI-TEHRANI A., PONTELL H., *Phishing Evolves*, cit., p. 319.
[265] Questa schematizzazione è seguita, ad es. da uno studio condotto dagli esperti dell'ITU- International Telecommunication Union, *Understanding Cyber crime: A Guide for Developing Country*, 2009, disponibile al sito https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf, p. 48.
[266] GERCHE M., *Internet-related Identity Theft*, pubblicato sul portale del Council of Europe, *Discussion Paper on Internet-related Identity Theft,* Strasburgo, 2007, disponibile al sito www.coe.int/cybercrime, p. 32.
[267] JOVER R.P., *Security Analysis of SMS as a Second Factor of Authentication: the challenges of multifactor authentication based on SMS, including cellular security deficiencies, SS7 exploits, and SIM swapping*, in *ACM queue*, 2020, vo. 18, n. 4, p. 37 ss., p. 52 ss.
[268] LEE K., KAISER B., MAYER J., NARAYANAN A., *An empirical study of wireless carrier authentication for SIM swaps*, atti del convegno *16th Symposium on Usable Privacy and Security*, disponibile *online* all'indirizzo https://www.ieee-security.org/TC/SPW2020/ ConPro/papers/lee-conpro20.pdf. *s*

aree o contenuti del suo computer, nonché i *worms*, tipologie di *malware* auto-replicante, che si propaga nei computer "infetti" al fine di prenderne il controllo da remoto. I *malware* oggi non vengono più installati unicamente sui *computer*, ma anche sugli *smartphone*. Negli ultimi tempi si sono diffusi i c.d. *mobile banking trojans*, ovvero *malware* di tipo *trojan*, diretti ad intercettare le credenziali delle App dei servizi di pagamento[269].

Altro fenomeno criminoso che causa notevoli perdite agli utenti e, più in generale, al sistema finanziario è il *carding*. Esso consiste nel furto (tramite *skimming*, ovvero posizionando un dispositivo capace di leggere e immagazzinare i dati in un apposito supporto[270]), nella rivendita e nell'indebito utilizzo dei dati delle carte di credito (o simili strumenti di pagamento) di ignare vittime[271]. I criminali informatici si dedicano alla raccolta dei dati delle carte di credito posizionando gli *skimmer* nei terminali di pagamento elettronici e microcamere ad essi vicini, così da scoprire anche il PIN degli utenti. Questo sistema non funziona unicamente con le carte di credito, potendo estendersi anche agli *account Paypal*. I dati delle carte di credito clonate vengono poi venduti sul *dark web* oppure in appositi gruppi *Telegram*, consentendo agli acquirenti di utilizzarli per fare acquisti illegali sui siti di *e-commerce*.

Per commettere questa tipologia di frodi è necessario carpire, in primo luogo, le informazioni personali della vittima, attività a sua volta illecita che sul *web* è più agevole compiere rispetto a quanto avviene nel mondo reale[272]. L'illecita sottrazione, detenzione e l'utilizzo di dati o codici identificativi di un soggetto vengono comunemente definiti come "furto d'identità" (o *identity theft*[273]). Tali fenomeni criminosi, anche se diretti ad ottenere un ingiusto profitto, coinvolgono anche la sfera intima e personale della vittima. In molti casi, con il furto d'identità, l'autore mira a far ricadere su persone inconsapevoli le conseguenze giuridiche (civili e penali) dei propri atti illeciti, garantendosi spesso l'impunità. Le menzionate tecniche hanno contribuito a mutare notevolmente il profilo delle frodi, portando alla creazione di un vero e proprio "mercato nero" di dati identificativi e personali

---

[269] V. il *Report* a cura dell'Europol, *Internet Organised Crime Threat Assessment (IOCTA)*, 2021, Luxembourg, p. 8, disponibile *online* all'indirizzo https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021#downloads

[270] KOCHHEIM D., *Cybercrime und Strafrecht der Informations- und Kommunikationstechnik*, München, 2018, p. 160 ss.

[271] LI W., CHEN H., NUNAMAKER J., *Identifying and Profiling Key Sellers in Cyber Carding Community: AZSecure Text Mining System*, in *Manag. Inf. Syst*., 2016, vol. 33, n. 4, p. 1059 ss., p. 1060.

[272] KIRK D., *Identifying Identity Theft,* in *J. Crim. Law*, 2014, vol. 78, n. 6, p. 448 ss., p. 449.

[273] OECD, *Scoping Paper on Online Identity Theft*, cit., p. 12; DE VRIES B., TIGCHELAAR J., VAN DER LINDEN T., *Describing Identity Fraud: Towards a Common Definition*, in *SCRIPTed*, 2008, vol. 5, n. 3, p. 482 ss., p. 495; BORGES G., SCHWENK J., STUCKENBERG C., WEGENER C., *Identitätsdiebstahl und Identitätsmissbrauch im Internet. Rechtlische und technische Aspekte*, Heidelberg, 2011, p. 10

delle vittime, che in questo modo diventano sempre più vulnerabili.

7. Estorsioni, impiego di *ransomware* e danneggiamenti informatici.

7.1. *Cyber extortion* e *sextortion*.

Molto diffuse negli ultimi anni sono le richieste estorsive. Queste ultime possono anche essere l'epilogo di una precedente truffa (v. *supra*, par. 4) in cui il reo, a seguito di una *romantic scam* ricatta la vittima minacciandola di divulgare le sue fotografie intime o i particolari della sua vita privata se non paga una determinata somma di denaro.

Sebbene estorsioni e minacce siano sempre esistite, le nuove tecnologie hanno consentito il loro proliferare, grazie all'anonimato che garantisce, almeno in parte, la rete. In tal senso, oggi si parla di *cyber extortion* per descrivere l'utilizzo di violenza o minacce *online* da parte dei criminali informatici al fine di costringere le vittime a consegnare loro denaro o altre utilità[274]. In alcuni casi si tratta di richieste estorsive che vengono inviate via *mail* o via *chat*, spesso nascondendosi dietro una falsa identità[275].

Di recente vi è stata una massiccia campagna di *spamming* a scopo estorsivo, nella quale un gruppo internazionale di criminali ha inviato diverse *e-mail* in cui veniva comunicato agli utenti che il loro *account* di posta elettronica era stato oggetto di attacco di tipo *hacking* e che in mancanza del pagamento di una determinata somma di denaro avrebbero subito gravissime conseguenze[276]. Negli ultimi tempi nei messaggi estorsivi i criminali fingono di appartenere alle forze dell'ordine e nelle loro *mail* sostengono che la vittima sarebbe indagata per "*pedopornografia, pedofilia, cyber pornografia, traffico sessuale*" e le intimano di pagare una determinata somma di denaro per chiudere l'indagine, altrimenti sarà arrestata[277]. Per spaventare la vittima, gli *hacker* utilizzano le credenziali degli utenti rese pubbliche a seguito di violazioni di dati o i loro dati personali che circolano sul *darkweb*. Per convincere le vittime a pagare, affermano falsamente di avere accesso alla *webcam*, al microfono e ad altri *software* sul loro dispositivo e che l'adozione di qualsiasi misura di sicurezza (come cambiare *password*) sarebbe inutile.

Del fenomeno della *cyber extortion* fa parte anche la *cyber sextortion*. In questo caso

---

[274] BOYCE B., *Cyber Extortion – The Corporate Response*, in *Comput. Secur*., 1997, n. 16, p. 25 ss., p. 25.
[275] LUBERTO M., "Sex-torsion" *via* web *e minaccia a mezzo* ransomware*: la nuova frontiera del delitto di estorsione*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (a cura di), *Cybercrime*, Torino, 2019, p. 724 ss., p. 727.
[276] https://www.commissariatodips.it/notizie/articolo/attenzione-nuova-campagna-di-spamming-a-scopo-estorsivo/index.html
[277] In argomento v. https://www.commissariatodips.it/notizie/articolo/attenzione-alle-false-email-di-organismi-di-polizia-1/index.html

i criminali informatici entrano in possesso di contenuti pornografici della vittima e la minacciano di divulgarli *online* se non paga una determinata somma di denaro o se non invia loro ulteriore materiale pornografico[278]. Peculiarità della *sextortion* è che l'azione può svolgersi integralmente *online*, senza che vi sia un contatto fisico tra autore del reato e vittima[279]. In alcuni casi, tali immagini sono state ottenute attivando illegalmente la *webcam* del computer della vittima; in altri casi, invece, tali immagini o video sono stati inviati dalla vittima nell'ambito di una precedente relazione sentimentale. Altre volte si tratta di un trucco psicologico, utilizzato dai criminali informatici per spaventare la vittima ed indurla a pagare una somma di denaro. Il fenomeno della *sextortion* coinvolge anche i minori, vittime ideali perché particolarmente vulnerabili e talmente preoccupati delle conseguenze di un'eventuale umiliazione pubblica sul *web* da essere propensi ad assecondare le richieste estorsive[280].

7.2. I *ransomware*.

Una tra le tipologie di *cyber extortion* più nota e pericolosa viene posta in essere mediante *ransomware*. Si tratta di un fenomeno complesso, composto da una fase di *hacking* e da una seconda fase nella quale viene fatta alla vittima una richiesta estorsiva. Il primo attacco mediante *ransomware* risale al 1989 e fu perpetrato mediante la consegna materiale di un *floppy disk* contenente un *malware* volto a criptare il *computer* della vittima, in cambio del pagamento di una somma in contanti[281]. Da allora tale tecnica si è notevolmente evoluta: con l'avvento del *web* non è più necessario intervenire fisicamente sul *computer* della vittima, dato che l'attacco può essere effettuato da remoto. Nel maggio del 2017 si diffuse a livello globale il *ransomware WannaCry*, infettando più di trecentomila *computer* in centocinquanta diversi Paesi, e costatò ai singoli utenti migliaia di dollari di riscatto e alle imprese ingenti perdite economiche[282]. Nel caso di attacchi *ransomware* il riscatto può essere chiesto in criptovalute oppure su piattaforme di pagamento *online*, garantendo l'anonimato della transazione[283]. Tali attacchi non colpiscono soltanto sistemi informatici, ma anche

[278] LIGGETT O'MALLEY R., HOLT K., *Cyber Sextortion: An Exploratory Analysis of Different Perpetrators Engaging in a Similar Crime*, in *J. Interpers. Violence*, 2022, vol. 37, n. 1-2, p. 258 ss., p. 261.
[279] *Ibid*.
[280] PATCHIN J.W., HINDUJA S., *Sextortion Among Adolescents: Results From a National Survey of U.S. Youth*, in *Sex. abuse*, 2020, vol. 32, n. 1, p. 30 ss., p. 35.
[281] SIMONE A., *The strange history of ransomware: Floppy disks, AIDS research, and a Panama P.O. Box.*, in *Medium*, 2015, disponibile al sito https://medium.com/un-hackable/the-bizarre-pre-internet-history-of-ransomware-bb480a652b4b.
[282] DELGADO-MOHATAR O., SIERRA-CÁMARA, ANGUIANO E., *Blockchain-based semi-autonomous ransomware*, in *Future Gener. Comput. Syst.*, 2020, vol. 112, p. 589 ss., p. 590.
[283] RYAN M., *Ransomware Revolution: The Rise of a Prodigious Cyber Threat*, Cham, 2021, p. 2.

singoli *smartphone*[284].

Il *ransomware* è un *malware* volto ad interrompere il funzionamento di un sistema informatico o ad impedire all'utente di accedere ai dati o di utilizzare un dispositivo o una rete[285]. I *ransomware* possono essere di due tipologie: mirati e non mirati. I primi sono rivolti ad un obiettivo specifico (ad es. un'istituzione pubblica), mentre i secondi sono costruiti per infettare indiscriminatamente il maggior numero possibile di sistemi informatici. Questi ultimi vengono diffusi tramite un *worm* (v. *supra*, par. 5), in modo da diffondersi e replicarsi in modo automatico nei sistemi infettati[286].

I *ransomware* possono essere diffusi nel computer delle vittime utilizzando le classiche tipologie di attacco informatico, tra cui le tecniche di *social engineering* (v. *supra*, par. 5.1). Il *phishing* è la tecnica prevalente per la diffusione dei *ransomware*[287]. Non è, però, necessario utilizzare tecniche di *social engineering*: grazie ai *crypto ransomware*, i criminali informatici studiano il sistema e ne sfruttano le vulnerabilità per diffondere il *malware*[288].

La procedura di infezione varia a seconda del vettore d'infezione utilizzato. Lo schema comune comprende tre fasi. Nella prima fase di *setup*, i criminali preparano quanto necessario per attuare l'attacco informatico, compromettendo in particolare una pagina *web* in cui installare il codice *exploit*, ovvero un codice, che identifica le vulnerabilità del sistema informatico. Nella seconda fase, c.d. di infezione, per cui chiunque visiti la pagina *web* precedentemente compromessa con un *browser* vulnerabile viene infettato. Nella pagina c.d. esca viene, infatti, incluso un piccolo frammento di codice autoinstallante (c.d. *dropper*), che scarica il codice binario del *ransomware* nel *computer*. Infine, la terza ed ultima fase è la c.d. *files encryption* (o crittografia dei file), nella quale il *ransomware* cripta tutti i *file* ritenuti di interesse nel computer della vittima[289]. In genere, le cartelle ed i *file* vengono bloccati (crittografati) e le immagini e i *file* di testo diventano blocchi di testo criptati, in modo tale che la vittima non possa usufruirne. Se il riscatto non viene pagato, il *ransomware* cagiona la perdita dei dati o la compromissione del funzionamento del *device* attaccato.

Esistono due tipologie di *ransomware*: i *locker ransomware* ed i *crypto ransomware*. I primi impediscono l'accesso ad un computer o ad un sistema informatico, bloccandone il

---

[284] MERCALDO F., NARDONE V., SANTONE A., VISAGGIO C.A., *Ransomware steals your phone. Formal methods rescue it,* in *36th IFIP WG 6.1 International Conference on Formal Techniques for Distributed Objects, Components, and Systems*, Heidelberg, 2016, p. 212 ss., p. 213.
[285] RYAN M., *Ransomware Revolution,* cit., p. 18.
[286] *Ibid*., p. 21.
[287] KSHETRI N., JEFFREY V., *Ransomware as a Business (RaaB),* in *IT Professional*, 2022, vol. 24, n. 2, p. 83 ss., p. 83, i quali evidenziano che nel 2021il *phishing* ha consentito la diffusione del 42% dei *ransomware*.
[288] *Ibid*., p. 85.
[289] DELGADO-MOHATAR O., SIERRA-CÁMARA, ANGUIANO E., *Blockchain-based,* cit., p. 590.

funzionamento. Poiché lasciano inalterata le funzionalità base del *Server*, gli esperti informatici sono in grado di rimuovere il *malware* e ripristinare la funzionalità del computer. I *crypto ransomware*, invece, impediscono l'accesso ai dati o ai *file*, bloccandoli o crittografandoli, non coinvolgendo il computer o il dispositivo di archiviazione nei quali sono contenuti[290]. Di quest'ultima tipologia fa parte anche il già citato *ransomware WannaCry*. Nel corso degli anni i creatori di *ransomware* hanno utilizzato e sperimentato differenti metodi di crittografia per criptare dati o sistemi informatici. Uno dei più utilizzati è l'algoritmo RSA, che si basa sull'esistenza di due chiavi distinte, una per la cifratura, l'altra per la decifratura. Esso consente di crittografare sia i dati contenuti nel *computer* della vittima, sia quelli contenuti nei dispositivi collegati alla rete locale[291]. Per ovviare ai problemi di lentezza che questo algoritmo presenta, è stata sviluppata una crittografia ibrida, che utilizza crittografia simmetrica e asimmetrica, ostacolandone la decifrazione[292]. A differenza dei *locker ransomware*, i *crypto ransomware* sono spesso irreversibili, in quanto le attuali tecniche di crittografia sono quasi impossibili da decifrare se implementate in modo appropriato[293].

Nel caso degli *scareware* i criminali utilizzano annunci *pop-up* per spaventare gli utenti facendogli credere che il loro *device* sia infetto e per questo motivo devono scaricare un determinato *software* antivirus[294]. Questa forma di *ransowmare* non blocca o danneggia direttamente il computer della vittima. Per questo motivo, viene classificata come tecnica di *hacking*, anziché come vera e propria terza tipologia di *ransomware*[295].

Particolarmente importante è il processo di notifica alla vittima dell'avvenuto attacco. Il *malware* è progettato per essere eseguito senza essere rilevato dal sistema attaccato, per cui è necessario portare a conoscenza della vittima che il sistema informatico è stato compromesso e le relative condizioni per il ripristino. Il codice maligno, di regola, viene progettato per fare in modo che sullo schermo del computer della vittima appaia un messaggio che la informa dell'avvenuto attacco di *hacking* accompagnato da una richiesta estorsiva per rendere nuovamente accessibile il sistema informatico, contenente i dettagli su come effettuare il pagamento ed i relativi termini per farlo[296]. Nella maggioranza dei casi,

---

[290] MABUNDA S., *Cyber Extortion, Ransomware and the South African Cybercrimes and Cybersecurity Bill*, in *Statute Law Rev*., 2019, vol. 40, n. 2, p. 143 ss., p. 145.
[291] O'KANE P., SEZER S., CARLIN D., *Evolution of ransomware*, in *IET Netw*., 2018, n. 7, p. 321 ss., p. 322.
[292] Aa. Vv., *Ransomware: Recent advances, analysis, challenges and future research directions*, in *Comput. Secur*, 2021, vol. 111, p. 1 ss., p. 2.
[293] *Ibid*.
[294] *Ibid*.
[295] *Ibid*.
[296] RYAN M., *Ransomware Revolution*, cit., p. 18.

come si è sottolineato, alle vittime viene richiesto di effettuare il pagamento del riscatto in *Bitcoin* a garanzia di anonimato, i quali vengono poi riciclati in modo tale da nasconderne la provenienza illecita[297]. In alcuni casi, i criminali cercano di spaventare la vittima, affermando falsamente di essere appartenenti all'autorità pubblica oppure fanno in modo che sullo schermo della vittima appaiano immagini pedopornografiche, minacciandole che se non provvedono immediatamente al pagamento saranno perseguite penalmente per il reato di pedopornografia[298]. Anche tale tipologia di attacchi informatici può avere epiloghi drammatici: in alcuni casi le vittime, spaventate dalle terribili conseguenze prospettate nei messaggi di richiesta di riscatto, si sono tolte la vita[299].

Diverse organizzazioni a delinquere, che diffondono *ransomware*, sono titolari di *Data Leak Site*, ovvero di siti presenti nel *darkweb*, nei quali sono custoditi i dati presenti nei computer delle vittime e che i criminali minacciano di pubblicare in caso di mancato pagamento del riscatto[300]. In alcuni casi i criminali informatici pretendono il pagamento di una somma supplementare per provvedere alla cancellazione dei dati[301]. A partire dal 2020 si è aggiunto un nuovo schema di *ransomware*, c.d. *triple extortion*: i criminali non si limitano a richiedere il denaro all'azienda cui hanno bloccato il *server*, ma anche a loro clienti e fornitori[302]. I criminali informatici hanno iniziato a sfruttare i servizi *Voice over Internet protocol* (VoIP) per contattare telefonicamente clienti e partner commerciali delle aziende colpite minacciandoli di pubblicare i loro dati in caso di mancato pagamento del riscatto. Spesso vengono sferrati ulteriori attacchi contro questi ultimi soggetti per spaventarli maggiormente[303].

Il recente sviluppo dei *ransomware* mostra un notevole incremento del fenomeno del *Ransomware-as-a-Service* (c.d. RaaS). Informatici professionisti mettono a disposizione le loro competenze a scopo criminale, facendosi pagare per sviluppare e diffondere un *ransomware* adatto a colpire obiettivi predefiniti dal committente[304]. In tale ambito è emersa l'esistenza di gruppi criminali che esaminano i siti di *social media* (ad esempio *LinkedIn*) per individuare i ruoli dei dipendenti e, quindi, scoprire quali sono gli utenti che hanno un accesso privilegiato al sistema. Dopodiché si occupano di carpire illecitamente le credenziali

[297] *Ibid*., p. 322.
[298] O'KANE P., SEZER S., CARLIN D., *Evolution of ransomware,* cit., p. 321.
[299] *Ibid*.
[300] KSHETRI N., JEFFREY V., *Ransomware as a Business,* cit., p. 83.
[301] *Ibid*.
[302] *Ibid*.
[303] V. il *Report* a cura dell'Europol, *Internet Organised Crime Threat Assessment,* cit., p. 21.
[304] RYAN M., *Ransomware Revolution,* cit., p. 144.

di autenticazione degli utenti (nomi utente e *password*) da un computer compromesso[305]. A tal scopo spesso rivolgono l'attacco informatico contro i servizi di *Remote Desktop Protocol* (RDP), che consentono ai dipendenti di lavorare a distanza[306]. I criminali informatici, o i committenti in caso di RaaS, utilizzano la richiesta di riscatto come pretesto per nascondere le reali motivazioni dell'attacco, che può essere sorretto da scopi politici oppure attuato a scopo vendicativo[307].

Gli attacchi *ransomware* continuano a coinvolgere soprattutto le piccole e medie imprese[308]. I danni, in termini economici, per le aziende sono molto elevati[309]. I pagamenti effettuati dalle singole vittime di tale estorsione non sono che una minuscola parte del costo complessivo di questi attacchi, dato che la produttività delle singole attività viene notevolmente compromessa, senza trascurare i costi per il ripristino del sistema danneggiato. Per questo motivo, il costo complessivo degli attacchi *ransomware* a livello globale è arrivato a toccare la cifra record di 20 bilioni di dollari USA per l'anno 2021[310].

7.3. I danneggiamenti informatici.

Oltre che a scopo estorsivo, i *malware* possono anche essere utilizzati per danneggiare un sistema informatico. Molto frequenti sono gli attacchi c.d. *Denial-of-Service Attack* (DoS), nei quali i criminali informatici danneggiano il sistema informatico altrui ostacolandone il corretto funzionamento o alterandone il suo corretto funzionamento, il quale, di conseguenza, non è più in grado di svolgere le funzioni per le quali è stato programmato. L'attacco può riguardare anche un *Server* di traffico Internet e in questo modo impedire agli utenti di accedere ai servizi e ai siti *online* ad esso collegati. Qualora tale attacco sia perpetrato tramite l'utilizzo di molteplici *device* interconnessi si parla di *Distributed Denial-of-Service Attack*[311].

I danneggiamenti informatici sono tornati in auge negli ultimi anni, a seguito del massiccio utilizzo di *malware* diretti a danneggiare i *Server* di infrastrutture critiche di un determinato Paese per influenzarne la politica, l'economia, ecc. Con l'informatizzazione dell'industria e dei servizi, un attacco informatico mirato può compromettere le infrastrutture

[305] KSHETRI N., JEFFREY V., *Ransomware as a Business*, cit., p. 85.
[306] *Ibid*., p. 84.
[307] KOCHHEIM D., *Cybercrime und Strafrecht*, cit., p. 128.
[308] SoSafe, *Report*, cit. p. 8.
[309] CONNOLLY A. Y., BORRION H., *Reducing Ransomware Crime: Analysis of Victims' Payment Decisions*, in *Comput. Secur*., 2022, vol. 119, p. 1 ss., p. 1.
[310] KSHETRI N., JEFFREY V., *Ransomware as a Business*, cit., p. 83.
[311] YU S., *Distributed Denial of Service Attack and Defense*, New York, 2014, p 1.

essenziali di un Paese. Gli attacchi diretti a danneggiare un sistema informatico in molti casi avvengono oggi nell'ambito del complesso fenomeno della *cyber warfare* (o guerra cibernetica), definita come l'azione di un Paese o un'organizzazione internazionale contro un altro Paese volta ad attaccare le reti e i sistemi informatici di quest'ultimo con l'obiettivo di interromperli, danneggiarli o distruggerli tramite virus informatici o attacchi *denial-of-service*[312].

Questo fenomeno ha mutato notevolmente la natura e la tipologia del danneggiamento. Se nel secolo scorso si riteneva che il danneggiamento tradizionale di cose fosse una mera offesa fine a se stessa, non in grado di denotare la pericolosità sociale dell'autore[313], oggi, nell'ambito cibernetico, la situazione è mutata. Dietro i danneggiamenti informatici non ci sono più soltanto delinquenti o piccoli criminali, ma dittature, organizzazioni a delinquere, associazioni a scopo terroristico, Stati, ecc. Il danneggiamento di tipo informatico, in tal senso, non è più visto come fine a se stesso, ma viene a costituire uno strumento per raggiungere scopi criminali o addirittura di guerra rivolti contro intere nazioni.

8. Il ruolo del soggetto passivo e la c.d. cifra oscura

Tradizionalmente si designa come vittima, *rectius* persona offesa, del reato il soggetto passivo, ovvero il titolare del bene offeso. Soggetto "passivo" giacché in ogni reato *persona duplice spectatur: ejus qui fecit et ejus qui passus est*[314].

La classificazione adottata dal codice penale Rocco nell'ambito dei delitti contro il patrimonio è tra offese inferte da una condotta unilaterale del reo e offese che si attuano con la cooperazione artificiosa della vittima. In tal senso, il soggetto passivo può limitarsi a subire il reato quale semplice spettatore, ovvero può contribuire a produrre il risultato patrimoniale pregiudizievole nei suoi confronti[315]. Nei casi in cui il reo sia l'artefice del processo lesivo, l'illiceità del fatto di reato scaturisce da un'aperta illegalità di forme e risultati. Diversamente, nelle figure di reato riconducibili allo schema della cooperazione tra reo e la sua "vittima", è quest'ultima a porre in essere l'atto di disposizione patrimoniale, mentre il disvalore del reato scaturisce dai mezzi impiegati per conseguire la cooperazione

[312] GOEL S., HONG Y., *Cyber War Games: Strategic Jostling Among Traditional Adversaries*, in Aa. Vv. (a cura di), *Cyber Warfare. Building the Scientific Foundation*, Cham, 2015, p. 1 ss., p. 3.
[313] SGUBBI F., *Uno studio*, cit., p. 196 ss.
[314] ROCCO A., *op. cit.*, p. 9 s.
[315] MANTOVANI F., *Contributo*, cit., p. 56.

"artificiosa"[316].

La menzionata classificazione appare oggi inadeguata ad abbracciare tutte le manifestazioni criminose poste in essere nel contesto cibernetico. Se la dottrina tradizionale riteneva incompatibile l'usurpazione unilaterale e la cooperazione artificiosa della vittima[317], le nuove tecniche informatiche o di aggressione al patrimonio hanno messo in evidenza i limiti di questo orientamento. Escluso il caso delle truffe su piattaforme di vendita *online* e le *advance fee fraud* (v. *supra*, par. 4), di regola la frode informatica si articola in più fasi, che partono dall'illecita intercettazione delle credenziali altrui, in cui l'apporto della vittima è indispensabile. A parte i casi limite nei quali il *computer* venduto alla vittima contenga già in sé il *malware*, solitamente è la "vittima" che, seppure inavvertitamente, navigando su un determinato sito *Internet*, connettendosi ad un terminale infetto o cliccando su un *link* di una *mail* di *phishing*, scarica sul suo dispositivo il programma maligno necessario per la commissione della frode informatica. In questi casi è il reo ad effettuare la disposizione patrimoniale a suo favore, ma riesce a far ciò grazie alla cooperazione artificiosa della vittima. Rimane, dunque, la cooperazione artificiosa, ma in questo caso non ricade sull'atto di disposizione patrimoniale, bensì riguarda una fase antecedente lo stesso.

Le statistiche indicano il fattore umano come responsabile del 90% dei reati informatici[318]. Le persone sono l'anello debole della sicurezza informatica e ne costituiscono la vulnerabilità principale. A tal proposito, si stima che l'uso improprio delle risorse di rete da parte dei dipendenti (c.d. *insider*) abbia contribuito a causare il 39% degli attacchi informatici subiti dalle aziende su un periodo di dodici mesi[319]. Sfruttare gli errori degli utenti in tema di *cybersecurity* è il modo più semplice per introdursi all'interno del sistema informatico di un'azienda. I casi più emblematici di criminalità informatica legata agli errori umani sono quelli di *social engineering*. Il mancato aggiornamento del sistema di sicurezza per negligenza può essere fonte di potenziali falle di sicurezza nel sistema. Con l'esponenziale aumento dello *smart working* durante la pandemia da Covid-19 si sono diffuse molti *Remote Desktop Protocol* e *Virtual private networks* per consentire ai dipendenti di lavorare da remoto. Conseguentemente, si sono abbassate le difese informatiche ed è stato più semplice per i criminali informatici penetrare nei *server* delle

[316] PEDRAZZI C., *Inganno ed errore*, cit., p. 40 ss.
[317] *Ibid*., p. 63.
[318] MENZE T., *The state of industrial cybersecurity*, *Report* per Kaspersky, 2019, p. 10, disponibile all'indirizzo https://ics.kaspersky.com/media/2019_Kaspersky_ARC_ICS_report.pdf.
[319] *Ibid*.

aziende[320].

Spesso la vittima non è in grado di accorgersi dell'attacco informatico in corso ed intervenire per bloccarlo. Non va dimenticato, infatti, che frequentemente il sistema *antivirus* non riesce a rilevare il *malware*, perché quest'ultimo è stato occultato. Eppure, anche se minimo, un contributo artificioso della vittima, quale ad esempio appoggiare la carta di credito al POS infetto oppure digitare le proprie credenziali mentre si è connessi ad una rete *Wi-Fi* non sicura, è sempre necessario. Questo contributo, però, non concerne la fase in cui il reo si impossessa del denaro della vittima, ma una fase antecedente. La fase dell'effettivo depauperamento patrimoniale del soggetto passivo, invece, si caratterizza per la totale assenza della sua collaborazione. Pare, dunque, che la tecnologia rompa la cooperazione tra autore e vittima caratterizzante i reati contro il patrimonio tradizionalmente classificati come quelli a cooperazione artificiosa della vittima, tra cui la truffa. Pertanto, il fenomeno della frode informatica finisce per porsi a metà strada tra la truffa ed il furto in una prospettiva di complessiva spersonalizzazione e patrimonializzazione della tutela[321].

Il fattore umano non sempre è preso in considerazione dada informatici e ingegneri nelle ricerche sulla *cybersecurity*[322]. Il ruolo delle "vittime" negli attacchi informatici non è affatto indifferente per il diritto penale. Tradizionalmente le fattispecie incentrate sulla condotta di sottrazione sono punite più severamente rispetto a quelle caratterizzate dal contributo del soggetto passivo all'evento dannoso, perché rivelano una pericolosità d'autore massima[323]. Tale classificazione, però, mal si adatta alla realtà odierna, dove, come si è visto, gli attacchi cibernetici contro il patrimonio sono di forma "ibrida". È difficile ritenere in tal senso che un *hacker* abbia una pericolosità sociale minore rispetto ad un comune ladro solo perché, per portare a buon fine l'attacco informatico, necessita della cooperazione artificiosa, spesso minima, da parte del soggetto passivo, peraltro nella fase antecedente l'effettiva sottrazione patrimoniale. Tuttavia, come si avrà modo di vedere meglio in seguito (v. *infra*, cap. III), la costruzione legislativa delle fattispecie penali volte a sanzionare gli attacchi informatici contro il patrimonio è modellata, almeno in parte, sulla falsariga delle fattispecie

---

[320] *The state of industrial security in 2022*, *Report* a cura dell'impresa di sicurezza informatica Barracuda Network, 2022, p. 23, disponibile *online* all'indirizzo https://www.barracuda.com/iiot-2022-report?utm_source=51231&utm_medium=blog&utm_campaign=blog.

[321] BARTOLI R., *La frode informatica tra "modellistica", diritto vigente, diritto vivente e prospettive di riforma*, in
Dir. informatica, 2011, n. 3, p. 383 ss., p. 384.

[322] MANCUSO V., STRANG A., FUNKE G.J., FINOMORE V.S., *Human factors of cyber attacks: a framework for human-centered research*, in *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 2014, vol. 58 n. 1, p. 437 ss., p. 439.

[323] SGUBBI F., *Uno studio*, cit., p. 153.

tradizionali. In tal senso, la frode informatica è modellata sulla fattispecie della truffa tradizionale[324], «*dalla quale si differenzia solo per il fatto che l'attività fraudolenta non investe la persona inducendola in errore, ma il sistema informatico di sua pertinenza attraverso una manipolazione*»[325]. Anche il trattamento sanzionatorio dei due reati, nell'ipotesi base, è rimasto identico, nonostante le diverse riforme che hanno riguardato il delitto di frode informatica. Ma, come si è visto, la realtà fenomenologica è molto diversa e in questo modo si finisce per equiparare casi tra loro disomogenei. Le frodi informatiche presentano elementi di complessità che le rendono autonome, sul piano strutturale, rispetto alle truffe tradizionali e questo dovrebbe, di conseguenza, riflettersi sul trattamento sanzionatorio, cosa che, ad oggi, non avviene. Ma anche le truffe *online*, seppur basate su schemi evoluti di truffe tradizionali, hanno aspetti peculiari. Basti solo pensare alla difficoltà relative all'identificazione delle persone che operano dietro l'anonimato garantito dal *web*, cosa che invece in una truffa compiuta integralmente nel mondo reale non avviene.

Le truffe *online* e le frodi informatiche sono tra i reati più diffusi in *Internet*, anche se le vittime sono più restie a denunciarli[326]. Questo perché la frode è uno dei pochi reati in cui è piuttosto comune che la vittima venga "colpevolizzata" per il reato subito[327]. Comunemente si ritiene che le vittime di *advance fee fraud* siano divenute tali perché si sono fatte accecare dalla loro avidità ed ingannare dalla loro credulità[328]. Per questo motivo, è piuttosto diffusa l'opinione per cui le vittime di tali reati dovrebbero essere considerate responsabili del "danno" subito, senza avere diritto ad alcun risarcimento[329]. Quest'orientamento, peraltro, ha portato all'elaborazione della teoria della c.d. vittimo-dogmatica, secondo cui non vi potrebbe essere reato quando la vittima, con i mezzi a propria disposizione, avrebbe potuto evitare l'inganno e, di conseguenza, l'evento lesivo[330]. Con

[324] PICOTTI L., *Sistematica dei reati informatici*, cit., p. 51.
[325] Cass. pen., sez. II, sentenza 24 novembre 2020, n. 32894; Cass. pen., sez. II, sentenza 17 marzo 2020, n. 10354.
[326] CROSS C., KELLY M., *The problem of "white noise": examining current prevention approaches to online fraud*, in *J. Financ. Crime*, 2016, vol. 23, n. 4, p. 806 ss., p. 807.
[327] Cft. GILLESPIE A.A., *The Electronic Spanish Prisoner*, cit., p. 221.
[328] CROSS C., *No laughing matter: blaming the victim of online fraud*, in *Int. Rev. vict*., 2015, vol. 21, n. 2, p. 187 ss., p. 192 e 193.
[329] Come riporta CROSS C., *Nobody's holding a gun to your head: Examining current discourses surrounding victims of online fraud*, in K. Richards, J. Tauri (eds.), *Crime, Justice and Social Democracy: Proceedings of the 2nd International Conference*, vol. 1, Brisbane, 2013, p. 25 ss., p. 30.
[330] In argomento v. SCHÜNEMANN B. *Strafrechtssystem und Betrug*, Herbolzheim, 2002; WALTHER S., *Eigenverantwortlichkeit und strafrechtliche Zurechnung: Zur Abgrenzung der Verantwortungsbereiche von Täter und "Opfer" bei riskantem Zusammenwirken*, Freiburg, 1991; FIEDLER R., *Zur Strafbarkeit der einverständlichen Fremdgefährdung: unter besonderer Berücksichtigung des viktimologischen Prinzips*, Frankfurt, 1990; HASSEMER R., *Schutzbedürftigkeit des Opfers und Strafrechtsdogmatik*, Berlin, 1981. Per la dottrina italiana v. DEL TUFO V., *Profili critici della vittimo-dommatica. Comportamento della vittima e delitto di truffa*, Napoli, 1990.

riferimento al reato di truffa, si è distinto tra "fiducia giustificata" (*der begründeten Vertrauen*), "fiducia necessaria" (*der notwendigen Vertrauen*) e "fiducia cieca" (*der blinden Vertrauen*)[331]. Solo le prime due forme di fiducia sarebbero meritevoli di tutela, poiché la fiducia che viene risposta in un altro soggetto senza una solida base di conoscenza, ovvero senza l'esistenza di fattori oggettivi che facciano apparire giustificato l'atteggiamento di fiducia, non sarebbe degna di tutela, dato che ciò contrasterebbe col principio di autoresponsabilità. Va, però, evidenziato che nel mondo virtuale è piuttosto difficile individuare quale possa essere una "solida base di conoscenza", visto che le persone sono tra loro in contatto attraverso uno schermo. Con riferimento specifico al *web* appare poi difficile individuare quali possano essere i fattori oggettivi sui quali basare la distinzione tra le diverse tipologie di fiducia.

Il giudizio negativo accomuna tutte le vittime di frodi informatiche, non solo quelle di truffe *online*, perché è piuttosto diffuso il sentimento per cui chi utilizza un *Server* o un terminale poco sicuro si merita di subire eventuali conseguenze negative[332], come se fosse facile sapere quando un terminale è stato manomesso. Da alcuni studi emerge che le vittime, nonostante le conseguenze negative da loro subite, non riuscirebbero a considerare quello da loro subito come un vero e proprio reato[333].

Questo non aiuta di certo la repressione di fenomeni criminosi complessi, dietro cui operano vere e proprie associazioni a delinquere e la colpevolizzazione delle vittime è un grosso ostacolo, poiché è uno dei fattori principali, unitamente alla scarsa fiducia nella giustizia, che le spinge a non denunciare l'accaduto[334]. Questi reati presentano un'elevata "cifra oscura", essendo scarsamente denunciati[335]. Gli studi hanno dimostrato che colpevolizzare la vittima per la sua ingenuità è comportamento tipico del criminale informatico, il quale cerca in questo modo di giustificarsi e minimizzare le sue responsabilità[336]. Addossare le "colpe" alla vittima ha un rilevante impatto anche per quanto riguarda la risocializzazione dei cybercriminali, che faticano a comprendere la portata lesiva

---

[331] ELLMER M., *Betrug und Opfermitverantwortung*, Berlin, 1986, p. 275 ss. Aderisce a tale tesi anche BOSCH S., *Straftaten in virtuellen Welten. Eine materiellrechtliche Untersuschung*, Berlin, 2018, p. 129, sostenendo che la stessa ben possa essere adattata al mondo virtuale.

[332] HUTCHINGS A., *Hacking and fraud: Qualitative analysis of online offending and victimization*, in K. Jaishankar, K. Routledge (a cura di), *Global Criminology: Crime and Victimization in the Globalized Era*, Cambridge, 2013, p. 93 ss., p. 110.

[333] V. NEREMBERG L., *Forgotten Victims of Financial Crime and Abuse: Facing the Challenge*, in *J. Elder Abuse Negl.*, 2000, vol. 12, n. 2, p. 49 ss., p. 50, che evidenzia come «*many victims fail to perceive financial crimes as crimes*».

[334] CROSS C., *No laughing matter*, cit., p. 191.

[335] CLUSIT, *Rapporto 2021*, cit., p. 9.

[336] HUTCHINGS A., *Hacking and fraud*, cit., p. 21 ss.

delle loro azioni e in questo modo sono propensi a reiterare tali comportamenti criminosi.

Le conseguenze psicologiche per le vittime di questi reati sono molto significative e possono coinvolgere anche la loro salute psico-fisica, con fenomeni depressivi e stress post-traumatico. Quando le perdite finanziarie sono ingenti, la vittima può finire in situazioni di povertà economica. In qualche caso, la vittima, sopraffatta dalle conseguenze negative, è arrivata a togliersi la vita[337]. Per questo motivo, alcuni studiosi hanno ritenuto che l'impatto delle frodi *online* sulle vittime possa essere paragonabile a quello dei reati violenti[338].

La truffa viene sanzionata perché sussiste sempre l'alterazione delle condizioni di eguaglianza e di libertà del consenso che uno dei contraenti effettua a scapito dell'altro[339]. Nelle truffe *online* e nelle frodi informatiche l'alterazione è portata ai massimi livelli. Non a caso le *advance fee fraud* oggi non vengono quasi più perpetrate inviando *e-mail* in massa, ma rivolgendosi ad uno specifico *target* di vittime vulnerabili, ricercate preventivamente in modo accurato sui *social network*. A tal proposito, è stato dimostrato che le potenziali vittime delle *online romance scams* vengono individuate in via preferenziale tra le persone che in precedenza hanno subito violenza domestica o sperimentato la rottura del matrimonio[340]. Si aggiunga poi che allo sviluppo della conoscenza delle vittime rispetto a tali fenomeni criminosi si accompagna di pari passo l'evoluzione delle tecniche messe a punto dai criminali informatici. Nelle *advance fee scams* raramente la richiesta di denaro avviene alla prima *mail*, ma è il seguito di una lunga frequentazione virtuale, durante la quale la vittima non ha mai modo di conoscere la reale identità chi si nasconde dietro allo schermo.

Nelle truffe e nelle frodi informatiche si è deciso di investire molto sulla prevenzione. Molti studi si concentrano sulle cause che spingono le vittime a rispondere ai messaggi fraudolenti e su come intercettare le potenziali vittime di questi reati[341]. Questo è senz'altro

---

[337] CROSS C., KELLY M., *The problem of "white noise"*, cit., p. 807. Più di recente v. la notizia di cronaca del 9 agosto 2022, riguardante un geometra veneto che dopo aver perso novecentomila euro ha tentato il suicidio. L'articolo è consultabile al sito https://www.ilgazzettino.it/nordest/treviso/bitcoin_criptovalute_geometra_risparmi_trading_online_truffa-6861013.html.

[338] Cft. DEEM D., *Notes from the field: observations in working with the forgotten victims of personal financial crimes*, in *J. Elder Abuse Negl*., 2000, vol. 12, n. 2, p. 33 ss., p. 36 ss.; NEREMBERG L., *Forgotten Victims of Financial Crime and Abuse*, cit., p. 36; CROSS C., *No laughing matter*, cit., p. 189.

[339] SGUBBI F., *Uno studio*, cit., p. 114.

[340] WHITTY M.T., *Is There a Scam for Everyone?*, cit., p. 401.

[341] V., a titolo esemplificativo, AA. VV., *Exploring how, why and in what contexts older adults are at risk of financial cybercrime victimisation: A realist review*, in *Exp. Gerontol*., 2022, vol. 159, p.1 ss.; BRANDS J., DOORN J.V., *The Measurement, Intensity and Determinants of Fear of Cybercrime: A systematic review*, in *Comput. Hum. Behav.*, 2022, vol. 127, p. 1 ss.; LEE C.S., *Online Fraud Victimization in China: A Case Study of Baidu Tieba*, in *Vict. Offenders*, 2021, vol. 16, n. 3, p. 343 ss.; NORRIS G., BROOKES A., DOWELL D., *The Psychology of Internet Fraud Victimisation: a Systematic Review*, in *J. Police Crim. Psychol.*, 2019, vol. 34, p. 231 ss.

corretto, ma non bisogna trascurare coloro che sono già divenute vittime di questi reati. Peraltro, come si è sopra esaminato, nelle frodi informatiche i criminali sviluppano tecniche sempre più sofisticate per carpire le credenziali o installare un *malware* nel computer della vittima e per organizzare una campagna pubblicitaria che metta in guardia gli utenti rispetto ad una determinata minaccia *online*. Solitamente occorre del tempo per studiare lo schema truffaldino, che nel frattempo avrà già colpito diversi utenti, ignari della portata della nuova minaccia cibernetica. Come si è visto in precedenza (v. *supra*, par. 5), in molti casi l'attacco informatico va a buon fine non tanto per la negligenza della vittima nel proteggere adeguatamente il suo *device*, ma le vulnerabilità del sistema utilizzato per le transazioni, (v., ad esempio, il caso dell'autenticazione via *Smartphone*). In alcuni casi sono i siti di *e-commerce* a non rispettare la normativa e a consentire le transazioni anche in mancanza dell'inserimento del PIN o di un altro fattore di autenticazione. In questo caso attribuire la responsabilità della frode unicamente alla vittima appare quantomai ingiusto. Il compito del diritto penale è proprio quello di stigmatizzare gli attacchi alle vittime deboli e allo stesso tempo aiutare a prevenirli, mentre le norme di diritto processuale penale devono tendere a tutelare la vittima nel processo[342]. Inoltre, queste nuove manifestazioni criminose non arrecano solo un danno patrimoniale alle persone, ma offendono anche interessi sopraindividuali (quali la tutela della pubblica fede, l'affidamento nei commerci, l'ordine pubblico economico, ecc.). Ad essere vittime di questi fenomeni criminosi non sono più i singoli cittadini o le aziende private, ma anche le infrastrutture pubbliche e le organizzazioni statali. Negli ultimi anni vi è stato un notevole incremento di attacchi diretti contro le infrastrutture critiche dei diversi Paesi. Considerare il tutto come una mera questione privata appare alquanto riduttivo. Pertanto, il ruolo delle vittime dev'essere sì tenuto in considerazione. Ed in tal senso occorre fare le opportune distinzioni, valorizzando le peculiarità di questi nuovi attacchi informatici, in modo da tutelare adeguatamente la vittima.

9. Le iniziative sovranazionali e gli obblighi di incriminazione europei in materia di *cybersecurity* e tutela dei mezzi di pagamento

Con lo sviluppo e la diffusione delle nuove tecnologie è emersa al contempo la necessità di proteggere le infrastrutture informatiche pubbliche e private dalle minacce dirette a lederne l'integrità. Ben presto ci si rese conto che il *cybercrime* è un fenomeno globale, che richiede una risposta comune a livello sovranazionale. A tal scopo, le istituzioni

[342] PAGLIARO A., *Tutela della vittima nel sistema penale delle garanzie*, in *Riv. it. dir. e proc. pen*., 2010, n. 1, p. 41 ss., p. 46.

europee avvertirono la necessità di un'azione congiunta a livello sovranazionale e, sin dagli anni '80 del secolo scorso, emanarono diversi provvedimenti per contrastare le nuove forme di criminalità riguardanti l'uso illecito delle nuove tecnologie.

Con la Raccomandazione del 9 settembre 1989, il Consiglio d'Europa adottò una "lista minima" di comportamenti da incriminare a livello nazionale. Rientravano in tale lista la frode informatica e falso informatico, danneggiamento di dati o programmi informatici, sabotaggio informatico, accesso e intercettazione non autorizzati. Nella "lista facoltativa" vennero, invece, inserite altre figure criminose, quali l'alterazione di dati o programmi informatici, lo spionaggio, l'utilizzazione non autorizzata di un elaboratore elettronico e l'utilizzazione non autorizzata di un programma informatico protetto[343]. Rispetto a queste ultime, era lasciata agli Stati parte del Consiglio d'Europa la scelta di ricorrere o meno allo strumento penale. La Raccomandazione recepiva le osservazioni contenute nel rapporto in materia di criminalità informatica, sviluppato da un gruppo di autorevoli esperti a livello europeo a metà degli anni '80 per conto dell'Organizzazione Europea per la Cooperazione e lo Sviluppo[344]. Per dare attuazione alla suddetta Raccomandazione, il nostro legislatore, con la l. 23 dicembre 1993, n. 547, introdusse, tra i primi in Europa, un articolato quadro di reati nel codice penale, per contrastare la criminalità informatica[345]. La successiva diffusione di *Internet* al pubblico, che ha comportato la c.d. rivoluzione cibernetica[346], favorì, oltre a nuove forme di sviluppo delle attività economiche, anche nuove forme di criminalità. In particolare, grazie all'interconnessione dei sistemi alla rete, molte attività, anche illecite possono essere svolte "da remoto", senza richiedere un contatto fisico con il *computer*. La peculiare architettura della rete, che garantisce, tra l'altro, la possibilità di agire coperti da anonimato, consentì il proliferare di condotte atte a danneggiare o mettere in pericolo l'integrità, la sicurezza e la riservatezza di dati e di sistemi informatici. La possibilità di agire attraverso il *web* consente all'autore del reato di agire anche da un luogo diverso rispetto a quello in cui si trova il computer della potenziale "vittima". Da questa situazione sorgono numerose difficoltà, perché il Paese in cui si trova l'autore del reato potrebbe non considerare

[343] Per un'analisi approfondita della R. (89)9 del CoE v. PICOTTI L., *Studi di diritto penale dell'informatica*, Verona, 1992, p. 23 ss. e 85 ss.
[344] OCSE, *Computer-Related Criminality: analysis of Legal Policy*, Parigi, 1986. In argomento v. SIEBER U., *The international Handbook on Computer Crime*, Chichester, 1986.
[345] Per l'analisi delle singole disposizioni e dell'iter legislativo v. SARZANA DI S. IPPOLITO C., *Informatica e diritto penale*, Milano, 1994, p. 197 ss.
[346] PICOTTI L., *Diritto penale e tecnologie informatiche: una visione d'insieme*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (a cura di), *Cybercrime*, cit., p. 33 ss., p. 36; WALDEN I., *Harmonising Computer Crime Laws in*
Europe, in *Eur. J. Crime Crim. Law Crim. Justice*, 2004, vol. 12, n. 4, p. 321 ss., p. 323 .

la condotta come un reato oppure potrebbe criminalizzarlo, ma come un reato minore punito con meno delle sanzioni minime per la cooperazione internazionale. Oppure, nonostante la presenza dei requisiti sanzionatori per la cooperazione, questa potrebbe non essere possibile perché i reati non soddisfano il requisito della doppia incriminazione[347].

Si avvertì, dunque, anche a livello europeo, la necessità di adottare un quadro giuridico a livello sovranazionale diretto ad armonizzare la risposta penale contro la criminalità cibernetica, favorendo al contempo le attività delle autorità di *law enforcement*[348].

9.1. La Convenzione *cybercrime*.

In tal senso, un ruolo cruciale è stato svolto dal Consiglio d'Europa. Di fondamentale importanza è la Convenzione *Cybercrime* del Consiglio d'Europa del 23 novembre 2001, sottoscritta da ben sessantotto Stati firmatari anche non appartenenti al COE, tra cui gli Stati Uniti d'America, il Giappone, la Nigeria, la Colombia, ecc. La Convenzione *Cybercrime* è ad oggi il principale strumento internazionale nell'ambito della criminalità cibernetica. La Convenzione non si limita a raccomandare agli Stati aderenti di punire i comportamenti in essa richiamati, ma prescrive loro di promuovere e adeguare gli strumenti processuali per le indagini investigative e la raccolta delle c.d. "prove elettroniche". In particolare, la Convenzione, oltre a fornire alcune definizioni terminologiche, identifica comportamenti illeciti per i quali tutti gli Stati aderenti dovrebbero prevedere sanzioni penali a livello interno. In tal senso, la Convenzione prescrive di punire l'accesso illegale, l'intercettazione illegale, attentato all'integrità dei dati e dei sistemi, abuso dei dispositivi, falsificazione informatica, frode informatica, pornografia minorile e violazioni del diritto d'autore[349]. La Convezione prevede che le sue disposizioni debbano applicarsi a tutti i reati commessi mediante un sistema informatico, nonché a qualsiasi altro reato di cui si debbano o possano raccogliere "prove in forma elettronica"[350]. Molto importante per comprendere la *ratio* delle disposizioni della Convenzione è l'*Official Explanatory Report*, vale a dire il rapporto esplicativo della Convenzione che, pur non essendo uno strumento di interpretazione autentica, riflette gli accordi delle parti raggiunti nella stesura della Convenzione ed è

[347] CALDERONI F., *The European legal framework on cybercrime: striving for an effective implementation*, in *Crime Law Soc Change*, 2010, vol. 54, p. 339 ss., p. 342.
[348] WALDEN I., *Harmonising Computer Crime Laws*, cit., p. 323.
[349] Per un'analisi delle singole disposizioni di parte generale v. PICOTTI L., *Internet e diritto penale: il quadro attuale alla luce dell'armonizzazione internazionale*, in *Dir. dell'Internet*, 2005, n. 2, p. 189 ss., p. 198 ss.
[350] V. art. 14, par. 2 della Convenzione: «*2. Salvo contraria disposizione risultante all'articolo 21, ogni Parte deve applicare i poteri e le procedure menzionati nel paragrafo 1.: a. ai reati previsti in conformità agli articoli da 2 a 11 della presente Convenzione; b. a tutti gli altri reati commessi attraverso un sistema informatico; c. all'insieme delle prove elettroniche di un reato*».

comunemente riconosciuto come base fondamentale per la sua interpretazione[351].

È proprio grazie alla Convenzione *Cybercrime* che molti Paesi europei hanno adottato a livello nazionale nuovi reati di accesso abusivo ad un sistema informatico e di intercettazione illecita di dati informatici[352]. Nel 2022 è stato siglato il secondo protocollo addizionale alla Convenzione, volto a rafforzare la cooperazione internazionale nella raccolta e divulgazione delle prove elettroniche[353]. Esso è destinato ad avere notevole rilevanza perché ad oggi manca ancora un quadro giuridico che disciplini la raccolta, la conservazione e lo scambio di prove digitali in tutti gli Stati membri dell'Unione europea.

9.2. La normativa dell'Unione europea.

L'Unione Europea, al pari del Consiglio d'Europa, si è mostrata sempre più attenta alle nuove forme di criminalità informatica e cibernetica e, nel corso del tempo, ha adottato diverse iniziative per contrastare e prevenire il *cybercrime* e garantire la *cybersecurity*.

A seguito dell'entrata in vigore del Trattato di Lisbona, la "criminalità cibernetica" è stata inserita nell'art. 83, par. 1, TFUE fra i fenomeni criminosi di natura grave e transnazionale su cui l'Unione europea ha competenza penale, seppur indiretta, potendo stabilire norme minime relative alla definizione dei reati e delle sanzioni[354].

Le fonti legislative dell'Unione europea maggiormente rilevanti ai fini della presente indagine sono la direttiva 2013/40/UE e la direttiva 2019/713/UE. A tutt'oggi, infatti, nonostante gli indubbi progressi, il legislatore europeo si dimostra ancora restio ad intervenire in materia penale.

In materia di frodi e falsificazioni di mezzi di pagamento diversi dai contanti, il primo atto adottato in seno all'Unione europea fu la decisione quadro 2001/413/GAI del Consiglio del 28 maggio 2001[355]. Il Consiglio dell'Unione europea aveva sottolineato che la gravità e

---

[351] MIQUELON-WEISSMAN M., *The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process?*, in *J. Marshall J. Computer & Info. L.*, 2005, vol. 23, n.2, p. 329 ss., p. 330.

[352] Per una panoramica sul recepimento degli artt. 2 e 3 della Convenzione *Cybercrime* da parte dei diversi stati europei v. PICOTTI L., SALVADORI I., *National Legislation implementing the Convention on Cybercrime-Comparative Analysis and Good Practices*, pubblicato sul portale del Council of Europe, *Working Paper,* Strasburgo, 2008, disponibile al sito www.coe.int/cybercrime.

[353] Per approfondimenti v. SPIEZIA F., *International cooperation and protection of victims in cyberspace: welcoming Protocol II to the Budapest Convention on Cybercrime*, in *ERA Forum*, 2022, vol. 23, n. 1, p. 101 ss.

[354] In argomento v. PICOTTI L., *Limiti garantistici delle incriminazioni penali e nuove competenze europee alla luce del Trattato di Lisbona*, in G. Grasso, L. Picotti, R. Sicurella, *L'evoluzione del diritto penale nei settori d'interesse europeo alla luce del Trattato di Lisbona*, Milano, 2011, p. 207 ss., p. 217 ss.

[355] L'obiettivo di tale Decisione quadro, che si inseriva in un quadro più ampio di disposizioni volte a costituire il c.d. diritto penale economico europeo, era quello di rafforzare ed armonizzare le disposizioni penali di beni e interessi attinenti alle istituzioni finanziarie comunitarie. Sul punto v. FOFFANI L., *Verso un'armonizzazione*

lo sviluppo di determinate forme di frode relative ai mezzi di pagamento diversi dai contanti esigevano soluzioni globali[356]. Tale atto legislativo è stato sostituito dalla citata direttiva 2019/713/UE, con la quale il legislatore europeo ha previsto obblighi di incriminazione concernenti le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti. L'obiettivo della direttiva consiste nell'armonizzare le diverse legislazioni penali degli Stati membri, in modo da contrastare in modo efficace un grave fenomeno transfrontaliero, che costituisce una seria minaccia per l'efficacia del mercato unico europeo[357].

Le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti non solo costituiscono una minaccia per la sicurezza cibernetica, dato che il denaro illecitamente sottratto alle vittime spesso viene impiegato per finanziare la criminalità organizzata, ma minano lo sviluppo del mercato unico digitale, poiché inducono i cittadini a diffidare dei nuovi strumenti digitali di pagamento. Il legislatore europeo ha scelto di intervenire in tale ambito prevedendo obblighi di incriminazione e prescrizioni per favorire lo scambio di informazioni e comunicazione dei reati, all'assistenza e al sostegno alle vittime e alla prevenzione.

La direttiva 2019/713/UE prevede che gli Stati membri puniscano comportamenti quali l'utilizzazione fraudolenta di strumenti di pagamento diversi dai contanti, nonché reati connessi quali il furto o altra illecita appropriazione, la contraffazione o falsificazione fraudolenta di tali strumenti, sia materiali che immateriali, il possesso di uno strumento di pagamento materiale rubato o altrimenti ottenuto mediante illecita appropriazione, o contraffatto o falsificato a fini di utilizzazione fraudolenta, nonché la frode connessa ai sistemi d'informazione. Inoltre, il legislatore europeo ha definito alcuni concetti chiave, quali, ad esempio, gli strumenti di pagamento diversi dai contanti, i mezzi di scambio digitale e la valuta virtuale, al fine di garantire uniformità nell'attuazione a livello nazionale delle direttive, nonché diverse disposizioni extrapenali, volte a garantire un'efficace cooperazione internazionale nel contrasto ai reati commessi contro gli strumenti di pagamento diversi dai contanti, quale ad esempio l'obbligatorietà della raccolta di dati statistici sulle frodi e sulle falsificazioni relative a strumenti di pagamento diversi dai contanti. Questa direttiva è stata recentemente attuata dal nostro legislatore col d.lgs. 8

europea del diritto penale dell'economia: la genesi di nuovi beni giuridici economici di rango comunitario, il ravvicinamento dei precetti e delle sanzioni, in G. Grasso, L. Picotti e R. Sicurella (a cura di), *L'evoluzione del diritto penale nei settori d'interesse europeo alla luce del Trattato di Lisbona*, Milano, Giuffrè, 2011, p. 583 ss., p. 584.

[356] V. il *Considerando* n. 1

[357] V. il *Considerando* n. 13 della direttiva 2019/713/UE. Per approfondire v. VADALÀ R.M., *La tutela penale della sicurezza degli scambi economici digitali*, 2021, disponibile al sito https://iris.univr.it.

novembre 2021 n. 184, il quale, come si esaminerà meglio in seguito (v. *infra*, cap. III), ha apportato alcune significative modifiche sia al codice penale che al d.lgs. 8 giugno 2001, n. 231, in materia di responsabilità da reato delle persone giuridiche.

Anche la direttiva 2013/40/UE, relativa agli attacchi contro i sistemi di informazione, prevede diversi obblighi di incriminazione allo scopo di garantire nello specifico il buon funzionamento e la sicurezza dei sistemi di informazione, fondamentali per lo sviluppo del mercato unico europeo, tramite l'armonizzazione delle legislazioni penali sostanziali. Tale direttiva, che ha sostituito la decisione quadro 2005/222/GAI, è stata emanata per ravvicinare il diritto penale degli Stati membri nel settore degli attacchi contro i sistemi di informazione, stabilendo norme minime relative alla definizione dei reati e delle sanzioni rilevanti. Essa persegue altresì il miglioramento della cooperazione fra le autorità competenti, compresi la polizia e gli altri servizi specializzati degli Stati membri incaricati dell'applicazione della legge, nonché le competenti agenzie e gli organismi specializzati dell'Unione (come Eurojust, Europol e il suo Centro europeo per la criminalità informatica, e l'Agenzia europea per la sicurezza delle reti e dell'informazione)[358]. L'art. 3 della direttiva prevede l'incriminazione dell'accesso illecito a sistemi di informazione, se avvenuto in violazione di una misura di sicurezza. L'art. 4 direttiva cit. prevede espressamente l'incriminazione delle condotte di "*ostacolare gravemente o interrompere il funzionamento di un sistema di informazione*", compiute anche "*rendendo inaccessibili i dati informatici*", mentre l'art. 5 direttiva cit. prescrive agli Stati di punire le medesime condotte, ma dirette nei confronti dei dati. L'art. 6, stabilisce l'obbligo per gli Stati membri di punire il fatto di intercettare senza autorizzazione le trasmissioni "*non pubbliche*" di dati informatici, a prescindere dal loro *contenuto* personale, riservato o segreto[359]. L'art. 7, infine, prevede l'adozione delle misure necessarie affinché la fabbricazione, la vendita, l'approvvigionamento per l'uso, l'importazione, la distribuzione o la messa a disposizione in altro modo intenzionali di uno degli strumenti ivi indicati per fini illeciti. Vi sono poi disposizioni extrapenali che prevedono lo scambio di informazioni tra gli Stati membri in relazione ai reati descritti dalla direttiva, nonché l'obbligo per questi ultimi di predisporre un sistema di registrazione, produzione e fornitura di dati statistici. Anche tale provvedimento, a seguito di un *iter*

[358] V. *Considerando* n. 1. In argomento v. CIVELLO CONIGLIARO S., *La nuova tutela penale europea dei sistemi di informazione. Una prima lettura della direttiva 2013/40/UE del Parlamento europeo e del Consiglio*, in *Dir. pen. cont.*, 30 ottobre 2013, p. 1 ss.
[359] SALVADORI I., *I reati contro la riservatezza informatica*, cit., p. 661.

particolarmente travagliato[360], è stato attuato dal nostro legislatore con l'art. 19 l. 23 dicembre 2021, n. 238 (v. *infra*, cap. II).

Il legislatore europeo si è dimostrato molto attento al fenomeno del reimpiego di capitali illeciti dato che, come sopra accennato (v. *supra* par. 3), i sistemi finanziari alternativi presenti sul *web*, e in particolare sul *dark web*, ben si prestano all'uso improprio per scopi criminali, favorito anche dall'anonimato strutturale di alcuni di essi (ad es. le criptovalute). Nel corso del tempo sono state emanate cinque direttive antiriciclaggio e numerosi provvedimenti in materia di prevenzione e contrasto del riciclaggio e del finanziamento del terrorismo. Vanno menzionate in questa sede la V direttiva antiriciclaggio 2018/843/UE, relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo, e la prima direttiva 2018/1673/UE sulla lotta al riciclaggio mediante il diritto penale, sul cui contenuto si avrà modo di tornare nel prosieguo (v. *infra*, cap. 4 par. 2), che prendono in considerazione i nuovi mezzi di pagamento e le valute virtuali.

In ambito europeo sono stati adottati diversi provvedimenti legislativi anche in materia di *cybersecurity*, definita come le attività necessarie per proteggere *network* e sistemi di informazione, i loro utilizzatori e le persone colpite dalle minacce cibernetiche[361].

Con il Regolamento CE 2004/460/CE fu istituita l'Agenzia europea per la sicurezza delle reti e dell'informazione (l'ENISA), col compito di supportare le istituzioni europee, gli Stati membri e gli operatori economici e contribuire ad assicurare un elevato livello di sicurezza delle reti e dell'informazione nella Comunità europea e a sviluppare una cultura in materia di sicurezza delle reti e dell'informazione a vantaggio dei cittadini, dei consumatori, delle imprese e delle organizzazioni del settore pubblico nell'Unione europea. Con il regolamento 2019/881/UE, il legislatore europeo ha investito l'Agenzia anche del compito di predisporre gli schemi di certificazione della sicurezza dei prodotti, servizi e processi informatici[362]. Oltre all'ENISA, nell'ambito dell'Unione europea opera anche l'*European*

[360] Inizialmente il legislatore italiano aveva comunicato alla Commissione europea che non vi era necessità di specifici interventi per attuare la direttiva, sostenendo che l'ordinamento nazionale fosse già conforme alle sue disposizioni. Tuttavia, la Commissione ha ritenuto che così non fosse ed ha aperto una procedura d'infrazione contro il nostro Paese per il mancato recepimento di tale normativa entro il termine previsto. Il legislatore italiano, dunque, ha deciso di intervenire con la citata legge europea 2019-2020. V. Dossier n. 294/2 del 13 aprile 2021, *Scheda di lettura della legge europea 2019- 2021* a cura dei Servizi e degli Uffici del Senato della Repubblica e della Camera dei deputati, disponibile *online* al seguente link: https://www.senato.it/japp/bgt/showdoc/18/DOSSIER/0/1210765/index.html?part=dossier_dossier1-frontespizio_front01.

[361] VAGENA E., NTELLIS P., *Cybersecurity Legislation: Latest Evolution in the EU and Their Implementation in the Greel Legal System*, in T. Synodinou, P. Jougleux, C. Markou, T. Prestitou (a cura di), *EU Internet Law in the Digital Era*, Cham, 2020, p. 239 ss., p. 240.

[362] V. art. 8 Regolamento (UE) 2019/881.

Cybercrime Centre (EC3), il quale a sua volta opera all'interno dell'Europol. L'EC3 riunisce le competenze europee in materia di criminalità informatica per sostenere le indagini degli Stati membri e funge da supporto operativo agli investigatori europei in materia di criminalità informatica, coordinando le operazioni e le indagini degli Stati membri, offrendo analisi e fornendo capacità di supporto tecnico e forense digitale altamente specializzate alle indagini e alle operazioni e supporto alle strutture di gestione delle crisi dell'UE. L'EC3 facilita inoltre la collaborazione operativa, tecnica e strategica tra le agenzie di contrasto (LEA) e le altre comunità informatiche pertinenti e le istituzioni, gli organi e le agenzie dell'UE (ad es. Eurojust, SEAE, ENISA, CERT-EU, Commissione, Consiglio, ecc.) e contribuisce alla preparazione e alla realizzazione di campagne e attività standardizzate di prevenzione e di sensibilizzazione nelle aree di competenza della criminalità informatica[363].

Di primaria importanza è la direttiva 2022/2555/UE, relativa alle misure per un livello comune elevato di cibersicurezza nell'Unione, c.d. NIS2. Essa abroga la direttiva 2016/1148/UE, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione ed il relativo Regolamento di esecuzione 2018/151/UE. Quest'ultima, oltre a stabilire obblighi di sicurezza e di notifica per gli operatori di servizi essenziali e per i fornitori di servizi digitali, obbligava gli Stati aderenti ad adottare una strategia nazionale in materia di sicurezza della rete e dei sistemi informativi. In particolare, essa prevedeva l'obbligo per gli Stati membri di provvedere affinché gli operatori di servizi essenziali notifichino senza indebito ritardo all'autorità competente o al CSIRT gli incidenti aventi un impatto rilevante sulla continuità dei servizi essenziali prestati. La direttiva, inoltre, ha istituito un gruppo di cooperazione al fine di sostenere e agevolare la cooperazione strategica e lo scambio di informazioni tra Stati membri e di sviluppare la fiducia tra di essi e ha creato una rete di gruppi di intervento per la sicurezza informatica in caso di incidente («rete CSIRT») per contribuire allo sviluppo della fiducia tra Stati membri e promuovere una cooperazione operativa rapida ed efficace. Il relativo Regolamento di esecuzione specificava ulteriormente gli elementi che i fornitori di servizi digitali devono prendere in considerazione nell'identificazione e nell'adozione delle misure volte a garantire un livello di sicurezza delle reti e dei sistemi informativi utilizzati, nonché precisato ulteriormente i parametri da prendere in considerazione al fine di determinare se un incidente abbia avuto un impatto rilevante sulla fornitura di tali servizi.

[363] https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.

Il nostro legislatore ha dato attuazione all'abrogata direttiva 2016/1148/UE col d.lgs. 18 marzo 2018, n. 65, e, da ultimo, col d.l. 21 settembre 2019, n. 105, conv. con modificazioni dalla legge 18 novembre 2019 n. 133, col quale è stato istituito il c.d. "*Perimetro di Sicurezza Nazionale Cibernetica*", volto ad assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati, aventi una sede nel territorio nazionale, da cui dipenda l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato[364].

La nuova direttiva 2022/2555/UE, entrata in vigore il 17 gennaio 2023, ha introdotto misure più stringenti e specifiche in termini di *cyber risk management*, di segnalazione e condivisione delle informazioni relative agli incidenti di sicurezza. In particolare, ha notevolmente ampliato il novero dei soggetti obbligati a rispettare gli obblighi di sicurezza, includendo anche ulteriori soggetti attivi in settori definiti "ad alta criticità", tra cui la gestione dei servizi ICT (*business-to-business*). La direttiva ha poi soppresso la vecchia distinzione tra "operatore di servizi essenziali" e di "fornitore di servizi digitali" ed ha suddiviso i soggetti obbligati in due nuove categorie, ovvero quella dei "soggetti essenziali" e quella dei "soggetti importanti". È stato poi riproposto l'obbligo di segnalazione degli incidenti, ma nel caso di "incidente significativo"[365] è stato previsto un particolare iter di notifica. Infine, particolarmente rilevanti sono le nuove previsioni in materia di vigilanza ed esecuzione cui sono sottoposti i soggetti obbligati ai sensi della direttiva, che prevedono la possibilità per l'autorità di sottoporre tali soggetti ad ispezioni o ad *audit*, nonché a sospensioni o divieti temporanei in caso di violazione delle disposizioni previste dalla direttiva.

La *cybersecurity* e la protezione dei dati personali sono strettamente correlati[366]. Molti dei fenomeni criminosi precedentemente descritti (v. *supra*, par. 5 e 6) coinvolgono il trattamento illegale dei dati personali delle vittime. In tale contesto, particolare rilevanza hanno assunto sia il Regolamento europeo sulla protezione dei dati personali (cd. *General Data Protection Regulation*) 2016/679/UE, che stabilisce norme generali per la protezione

[364] V. PICOTTI L., *Cybersecurity: quid novi?*, in *Dir. di Internet*, 2020, n. 1, p. 11 ss., p. 13; MELE S., *Il Perimetro di Sicurezza Nazionale Cibernetica*, ivi, p. 15 ss., p. 15.
[365] L'art. 23 della direttiva specifica che: «*un incidente è considerato significativo se: a) ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato; b) si è ripercosso o è in grado di ripercuotersi su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli*».
[366] VAGENA E., NTELLIS P., *Cybersecurity Legislation*, cit., p. 255.

delle persone fisiche in relazione al trattamento dei dati personali e per la libera circolazione di questi ultimi nel territorio dell'Unione e delle direttive 2016/680/UE e 2016/681/UE. La prima direttiva menzionata riguarda la protezione delle persone fisiche in riferimento al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati, mentre la seconda è relativa all'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi. L'ambito di applicazione delle menzionate direttive è limitato ai settori della cooperazione giudiziaria in materia penale e della cooperazione di polizia. L'adeguamento della normativa nazionale ai tre atti legislativi sopra menzionati ha avuto impatto anche sulla normativa penale dei diversi Stati membri (v. *infra*, cap. II, par. 8 e cap. V, par. 3).

Occorre, infine, menzionare, ai fini della presente ricerca, anche il Regolamento 910/2014/UE c.d. eIDAS *(acronimo di Electronic Identification, Authentication, Signature*) in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno. Si tratta di uno dei principali atti legislativi europei in materia di *e-commerce*[367]. L'esigenza di garantire la certezza sull'identità altrui è particolarmente sentita per quanto riguarda le transazioni *online.* In tal senso, lo scopo di questo regolamento è di assicurare un livello adeguato di sicurezza dei mezzi di identificazione elettronica e dei servizi fiduciari, istituendo un quadro giuridico comune per le firme elettroniche, i sigilli elettronici, le validazioni temporali elettroniche, i documenti elettronici, i servizi elettronici di recapito certificato e i servizi relativi ai certificati di autenticazione di siti *web*.

Il legislatore europeo ha adottato numerose disposizioni legislative volte garantire la sicurezza delle reti e dei servizi di comunicazione elettronica e, di conseguenza, accrescere la fiducia dei cittadini europei nel mercato digitale. Come si esaminerà in seguito, molti di questi provvedimenti sono stati attuati dai legislatori nazionali (tra cui il nostro), attraverso l'introduzione di nuove fattispecie incriminatrici e/o la riformulazione di quelle già esistenti. La previsione di definizioni e, in alcuni casi, di veri e propri obblighi di incriminazione da parte del legislatore europeo ha, dunque, contribuito ad armonizzare le legislazioni degli Stati membri, i quali hanno provveduto ad inserire nuovi reati per sanzionare i comportamenti criminosi descritti. Tuttavia, nonostante gli indubbi progressi, permangono ancora significative differenze tra le legislazioni nazionali in materia di criminalità

[367] Per approfondire v. ZACCARIA A., SCHMIDT-KESSEL M., SCHULZE R., GAMBINO A.M. (a cura di), *EU eIDAS Regulation. Article-by-Article Commentary*, München, 2020.

cibernetica. Non può dirsi pertanto ancora raggiunta una piena armonizzazione *in subiecta materia*. Questo rischia di compromettere la lotta a tali manifestazioni criminose, le quali, avvengono, di regola, a livello sovranazionale, dal momento che notevoli differenze a livello sanzionatorio ostacolano la cooperazione tra i diversi Stati membri.

10. Considerazioni di sintesi

Il *cybercrime* è un fenomeno complesso, in continua evoluzione e tutt'altro che prevedibile. Gli attacchi informatici contro il patrimonio, sferrati nella maggioranza dei casi da associazioni a delinquere di carattere transnazionale (v. *supra*, par. 4.1), causano ingenti perdite economiche al sistema finanziario e creditizio, notevoli danni d'immagine agli istituti di credito, e significativi danni (anche psicologici) alle vittime. Essi, infatti, sono particolarmente insidiosi non soltanto per quanto riguarda l'individuazione degli autori del reato, che quasi sempre sfruttano l'anonimato del *web* per celare le loro reali identità, ma soprattutto per le vittime, le quali non hanno cognizione immediata dell'evento lesivo[368] e spesso subiscono anche gravi conseguenze socio-psicologiche a seguito della scoperta della propria vulnerabilità. Pertanto, ad essere leso non è unicamente il bene giuridico del patrimonio, ma anche altri beni giuridici quali l'integrità, la sicurezza informatica e la riservatezza informatica.

Come è emerso nel presente capitolo, i criminali informatici hanno notevolmente affinato le loro tecniche ed hanno sperimentato e perfezionato nuove tecniche per derubare le vittime sfruttando le nuove tecnologie informatiche e il sempre più diffuso utilizzo dei nuovi strumenti di pagamento. Inoltre, oggi hanno anche la possibilità di sfruttare l'intelligenza artificiale per i loro scopi illeciti. Significativa, poi, è l'affermazione del *Cybercrime-as-a-service*, per cui non è più necessario per il criminale informatico possedere specifiche conoscenze tecnico-informatiche, dato che può acquistare *malware*, *bootnet*, ecc. preconfezionati.

Le nuove tecniche, inoltre, hanno messo in crisi la tradizionale classificazione dei reati contro il patrimonio tra quelli commessi mediante furto e mediante frode. Come si è visto, la menzionata classificazione appare oggi inadeguata ad abbracciare tutte le manifestazioni criminose poste in essere nel contesto cibernetico.

---

[368] GERCHE M., *Internet-related Identity Theft*, pubblicato sul portale del COUNCIL OF EUROPE, *Discussion Paper on Internet-related Identity Theft,* Strasburgo, 2007, disponibile *online* al sito www.coe.int/cybercrime.

Nonostante le conseguenze lesive del fenomeno, che coinvolge sempre più anche i sistemi informatici dello Stato, i criminali informatici responsabili di tali attacchi vengono effettivamente perseguiti penalmente in un numero molto limitato di casi e del tutto marginale è l'incidenza delle frodi informatiche nelle statistiche giudiziarie relative alle condanne. A tal scopo, l'Unione Europea, e il Consiglio d'Europa si sono dimostrate istituzioni attente alle nuove forme di criminalità informatica e cibernetica e, nel corso del tempo, hanno adottato diverse iniziative per contrastare e prevenire il *cybercrime* e garantire la *cybersecurity*. Molti di questi provvedimenti sono stati attuati dai legislatori nazionali, attraverso l'introduzione di nuove fattispecie incriminatrici e/o la riformulazione di quelle già esistenti, che saranno esaminate nel corso del presente lavoro.

Capitolo II

L'incriminazione di meri atti preparatori alla commissione di più gravi reati *lato sensu* patrimoniali

Sommario: 1. L'anticipazione della tutela penale al vaglio dei principi di proporzionalità e offensività.; - 1.1. La problematica dei *dual-use software*. - 2. Il reato di accesso abusivo ad un sistema informatico o telematico di cui all'art. 615-*ter* c.p. - 3. Il reato di detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici di cui all'art. 615-*quater* c.p. – 4. I rapporti concorsuali. - 5. Il nuovo reato di detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti di cui all'art. 493-*quater* c.p. - 6. La detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico di cui all'art. 615-*quinquies* c.p. - 7. La rilevanza penale delle intercettazioni informatiche. – 8. Il reato di sostituzione di persona di cui all'art. 494 c.p. – 9. Le norme incriminatrici contenute nel c.d. codice della *privacy*. - 10. La controversa rilevanza penale del "furto di dati" e della "ricettazione di dati". – 11. La difficile individuazione dei rapporti tra le norme incriminatrici. – 12. Considerazioni di sintesi.

1. L'anticipazione della tutela penale al vaglio dei principi di proporzionalità e offensività.

Come già avuto modo di evidenziare in precedenza (v. *supra*, cap. I, par. 9), il legislatore introdusse per la prima volta nel nostro ordinamento apposite fattispecie incriminatrici *ad hoc* volte a reprimere la c.d. criminalità informatica con la l. 23 dicembre 1993 n. 547. In tale occasione, scelse di non riunire le nuove fattispecie in un unico titolo o capo autonomo del codice penale, bensì di ricondurle alle figure tradizionali ritenute affini, ovvero di collocarle accanto ad esse. Per tale motivo, la nuova fattispecie di frode informatica fu collocata accanto a quella di truffa di cui all'art. 640 c.p., mentre altre disposizioni (tra cui l'accesso abusivo a sistema informatico o telematico e le fattispecie relative alle intercettazioni informatiche) furono collocate rispettivamente nella sezione IV, relativa ai delitti contro l'inviolabilità del domicilio, e nella sezione V, concernente i delitti contro l'inviolabilità dei segreti, del Titolo XII del Libro II del codice penale. Secondo il legislatore del 1993, tale scelta si giustificava perché i nuovi fenomeni criminosi commessi

mediante o contro le tecnologie informatiche rappresentavano solo una diversa modalità di aggressione ai beni giuridici tradizionali[1]. La menzionata scelta legislativa ebbe, almeno in parte, il pregio di rispettare il tradizionale criterio di classificazione dei reati[2], incentrato sul bene giuridico protetto. Non mancarono, tuttavia, le critiche[3], poiché tale scelta influenzò la formulazione delle nuove norme incriminatrici, le quali vennero costruite sulla falsariga delle fattispecie tradizionali già esistenti, in molti casi utilizzando la stessa terminologia. Non si tenne conto così della difficoltà di far rientrare fatti, condotte e oggetti del tutto nuovi (e profondamente diversi) in schemi concepiti per realtà differenti[4]. La scelta in esame causò altresì un'estrema frammentazione della disciplina, che all'atto pratico determinò la moltiplicazione delle fattispecie incriminatrici applicabili a molti dei fenomeni criminosi emergenti (come ad esempio il *phishing*).

Questa moltiplicazione è stata ulteriormente aggravata a seguito delle recenti riforme, ed in specie con quelle di cui al d.lgs. 8 novembre 2021 n. 184 e alla l. 23 dicembre 2021, n. 238. Quando, per dare attuazione alle prescrizioni di fonte sovranazionale, si è reso necessario modificare i reati informatici introdotti nel 1993, il nostro legislatore è intervenuto soltanto su un limitato gruppo di fattispecie, senza considerare la stretta correlazione esistente tra i diversi gruppi di norme incriminatrici. Come si esaminerà nel prosieguo (v. infra, par. 11), si è così prodotta una farraginosa sovrapposizione di incriminazioni.

---

[1] Cft. Camera dei Deputati, XI Legislatura, disegno di legge n. 2733, *Presentazione del Ministro di Grazia e Giustizia (Conso)*, disponibile al sito http://legislature.camera.it, nella parte in cui si evidenzia che: «*un primo problema è nato a seguito della scelta, nell'ambito del più ampio disegno di politica penale volto ad arginare la sempre più ampia tendenza alla decodificazione, di modificare il codice penale e di non promuovere una legge penale speciale. È stato necessario, quindi, stabilire se le nuove figure di reato da introdurre nel codice penale dovessero essere inserite in un apposito titolo del libro II […] da destinare esclusivamente ad esse; o se, invece, fosse preferibile ricondurre i nuovi reati alle figure già esistenti che ad essi, pur nella loro autonomia, appaiano più vicine. Si è ritenuta preferibile la seconda soluzione, nella convinzione che la particolarità della materia non costituisse ragione sufficiente per la configurazione di uno specifico titolo; d'altra parte, il criterio seguito dal legislatore del 1930 nel prevedere i vari raggruppamenti dei reati è ispirato all'unità dell'oggetto giuridico, inteso quanto meno come unico interesse di categoria, mentre le figure da introdurre sono apparse subito soltanto quali nuove forme di aggressione, caratterizzate dal mezzo o dall'oggetto materiale, ai beni giuridici (patrimonio, fede pubblica, eccetera) già oggetto di tutela nelle diverse parti del corpo del codice*».

[2] V. PICOTTI L. voce *Reati informatici*, in *Enc. giur. Treccani*, VIII agg., Roma, 1999, p. 1 ss., p. 5; BERGHELLA F., BLAIOTTA R., *Diritto penale dell'informatica e beni giuridici*, cit., p. 2330, i quali evidenziano che la scelta in questione «*ha inoltre consentito di non disperdere il complesso lavorio dottrinale e giurisprudenziale che aveva tentato la collocazione delle stesse fenomenologie entro le figure del diritto penale tradizionale*». Più in generale, sulla funzione classificatoria del bene giuridico v., per tutti ANGIONI F., *Contenuto e funzioni del concetto di bene giuridico*, Milano, 1983, p. 11 ss.

[3] Così anche BUSSOLATI N., *Accesso abusivo a un sistema informatico o telematico ex art. 615-ter c.p.: il nodo* dell'abusività, in *Stud. Iuris*, 2018, n. 4, p. 428 ss., p. 429; nonché PICOTTI L., *Sistematica*, cit., p. 53; BERGHELLA F., BLAIOTTA R., *Diritto penale dell'informatica e beni giuridici*, cit., p. 2330.

[4] PICOTTI L., *Sistematica*, cit., p. 53; SALVADORI I., *L'accesso abusivo ad un sistema informatico*, cit., p. 131.

Il legislatore del 1993 aveva compreso che la criminalità informatica non poteva essere considerata unicamente come una manifestazione della criminalità economica. Paradigmatica è la previsione dell'art. 615-*ter* c.p., che fu inserito nel codice penale proprio per tutelare lo *jus excludendi alios* rispetto a determinati spazi virtuali[5], a prescindere dalla presenza di un danno patrimoniale per il suo titolare o il suo fruitore. Lo stesso dicasi per l'art. 615-*quater* c.p., mediante il quale si punì la diffusione di codici e altri mezzi atti all'accesso a sistemi informatici o telematici, disposizione che non era prevista neppure nella c.d. "lista facoltativa" della Raccomandazione del 1989.

È, quindi, evidente l'intrinseca strumentalità dei citati reati informatici rispetto alla tutela di ulteriori beni giuridici, quali quelli protetti dal delitto di frode informatica o dai reati contro i danneggiamenti informatici. La stessa disposizione di cui all'art. 615-*ter* c.p. sanziona una condotta prodromica alla commissione di ulteriori reati, in quanto è assai raro che l'accesso abusivo ad un sistema informatico sia fine a se stesso. Ma l'eccessiva anticipazione della tutela penale porta con sé alcuni inconvenienti e può collidere con alcuni fondamentali principi penalistici (di offensività, proporzionalità e sussidiarietà). Paradigmatici sono, come si esaminerà più approfonditamente nei successivi paragrafi (v. *infra*, par. 3, 6 e 7), i casi in cui la soglia dell'intervento penale viene anticipata al punto da punire comportamenti tali da costituire soltanto un pericolo indiretto per beni giuridici di rango secondario[6].

Il principio di offensività impone al legislatore di punire soltanto comportamenti tali da ledere o quantomeno mettere in pericolo beni giuridici[7]. In dottrina prevale la tesi secondo cui oggetto di tutela penale sono non solo i beni costituzionalmente rilevanti, ma anche quelli non contrastanti con la Costituzione[8]. In questo senso, il bene giuridico tutelato della riservatezza informatica appare senz'altro costituzionalmente compatibile, dato che lo stesso

[5] Cft. la Relazione del Disegno di legge n. 2773, cit., p. 9, ove si evidenzia che «*la normativa trova la sua collocazione tra i reati contro l'inviolabilità del domicilio perché i sistemi informatici o telematici, la cui violazione essa reprime, costituiscono un'espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantito dall'articolo 14 della Costituzione e penalmente tutelata nei suoi aspetti più essenziali e tradizionali agli articoli 614 e 615 del codice penale*».

[6] PECORELLA C., *Il diritto penale dell'informatica*, cit., p. 360.

[7] MANTOVANI F., *Il principio di offensività del reato nella Costituzione*, in *Scritti in onore di Costantino Mortati*, vol. IV, Milano, 1977, p. 447 ss., p. 447.

[8] Per tutti v. PULITANÓ D., *Bene giuridico e giustizia costituzionale*, in A.M. Stile (a cura di), *Bene giuridico e riforma della parte speciale*, Napoli, 1985, p. 133 ss., p. 136 ss.; MANTOVANI F., *Il problema della offensività del reato nelle prospettive di riforma del codice penale*, in G. Vassalli (a cura di), *Problemi generali di diritto penale. Contributo alla riforma*, Milano. 1982, p. 63 ss., p. 67; MANES V., *Il principio di offensività nel diritto penale. Canone di politica criminale, criterio ermeneutico, parametro di ragionevolezza*, Torino, 2005, 74 ss. e 209 ss.; DONINI M., *Il principio di offensività. Dalla penalistica italiana ai programmi europei*, in *Riv. trim. dir. pen. cont.*, 2013, n. 4, p. 4 ss., p. 17.

appare riconducibile all'art. 7 della Carta di Nizza, che riconosce il rispetto alla vita privata intesa in senso lato, nonché all'art. 8 della Convenzione Europea dei Diritti dell'Uomo[9]. Tuttavia, qualche autore ha affermato che ciò non è sufficiente a giustificare l'arretramento della soglia dell'intervento penale, poiché si evidenzia che la tutela dei dati immagazzinati in un sistema informatico non è un bene di rango primario o comunque «*indispensabile per l'integrità delle istituzioni e per la sopravvivenza stessa della società*»[10]. Va però rilevato che questa affermazione risale ad un'epoca in cui l'utilizzo delle moderne tecnologie informatiche e della rete non era così massiccio e pervasivo come quello odierno. Oggi, infatti, il funzionamento di moltissime infrastrutture statali si regge su sistemi informatici e, come dimostrato dalla cronaca recente[11], un attacco *ransomware* diretto contro il sistema informatico di un'infrastruttura critica, quale ad esempio il sistema ferroviario o sanitario, può paralizzare intere strutture pubbliche rendendo quel servizio pubblico non fruibile anche per giorni interi. Non appare dunque esagerato affermare che oggi l'integrità e la riservatezza dei dati immagazzinati in un sistema informatico, interessi strettamente correlati tra loro dato che la sicurezza dei dati dipende dalla loro riservatezza, siano effettivamente indispensabili per l'integrità delle istituzioni e la sopravvivenza della società.

L'esistenza di un bene giuridico meritevole di tutela non è di per sé sufficiente a giustificare l'introduzione di un reato, poiché deve sussistere anche l'effettiva necessità (o "bisogno") di ricorrere allo strumento penale per punire meri atti prodromici o preparatori alla commissione di più gravi reati[12]. Il principio di proporzionalità impone al legislatore di adottare mezzi adeguati rispetto al fine prefissato, recando il minor sacrificio possibile a coloro che ne subiscono gli effetti[13]. Tanto più importante è il bene da tutelare, quanto più è legittimo anticipare l'intervento penale[14]. Ritornando all'ambito della criminalità cibernetica, data l'importanza dei beni giuridici da tutelare e il trattamento sanzionatorio non

[9] PICOTTI L., *Nuove tecnologie e beni giuridici della persona*, in ID (a cura di), *Tutela penale della persona e nuove tecnologie*, Padova, 2013, p. 29 ss., p. 62.
[10] PECORELLA C., *Il diritto penale dell'informatica*, cit., p. 360.
[11] V., a titolo di esempio, l'attacco *ransomware* che, in data 23 marzo 2022, ha colpito i *Server* della rete Trenitalia/Ferrovie dello Stato bloccando per giorni interi la vendita biglietti in stazioni, nelle biglietterie e *self-service*:
https://www.repubblica.it/tecnologia/2022/03/24/news/trenitalia_assaltata_dagli_hacker_di_hive_group_vogliono_5_milioni_di_dollari-342626658/
[12] ROMANO M., *"Meritevolezza di pena", "bisogno di pena" e teoria del reato*, in *Riv. it. dir. proc. pen*., 1992, n. 1, p. 39 ss., p. 50.
[13] Sul principio di proporzione v. per tutti ANGIONI F., *Contenuto e funzioni del concetto di bene giuridico*, cit., p. 164 ss. Nella dottrina tedesca v. ROXIN C., *Kriminalpolitik und Strafrechtssystem*, Berlin, 1973, p. 26. Sulla distinzione tra principio di offensività e proporzionalità v. DONINI M., *Il principio di offensività*, cit., p. 18 ss.; MANES V., *Il principio di offensività nel diritto penale*, cit., p. 137 ss.
[14] ANGIONI F., *Contenuto e funzioni del concetto di bene giuridico*, cit., p. 176.

particolarmente severo previsto per tali reati (gli artt. 615-*quater*, 615-*quinquies* e 493-*quater* c.p. sono puniti con la reclusione fino a due anni) non appare esservi contrasto col principio di proporzionalità.

In base al principio di sussidiarietà (o *extrema ratio*) la sanzione penale può essere adottata soltanto in presenza dell'offesa di un bene che, seppur non sia di pari grado rispetto all'interesse sacrificato (ovvero la libertà personale), sia almeno dotato di rango costituzionale[15]. Corollario del principio di sussidiarietà è il principio di frammentarietà del diritto penale, in forza del quale non si devono punire tutte le condotte lesive del bene giuridico protetto, ma solo le modalità di aggressione più pericolose[16].

I menzionati principi finiscono per incidere anche sul ricorso alla sanzione penale, la quale deve essere determinata dal legislatore in base ad un criterio di proporzione, sia di sussidiarietà[17].

Il principio di frammentarietà non appare essere stato debitamente tenuto in considerazione nell'ambito dei reati informatici posti a tutela del patrimonio e della riservatezza informatica. Con l'ultima riforma di cui alla l. 23 dicembre 2021, n. 238, il legislatore ha esteso in modo eccessivo l'ambito di applicazione di molte fattispecie a tutela della riservatezza informatica e quelle concernenti le intercettazioni informatiche. La ragione di tale scelta pare, almeno in parte, risentire della formulazione delle direttive europee a cui le citate novelle hanno dato attuazione. Le direttive prevedono un'ampia lista di condotte da incriminare, peraltro a volte con significato simile (ad es. "*il danneggiamento,*

---

[15] BRICOLA F., *Teoria generale del reato*, in *Noviss. Dig. it.*, vol. XIX, Torino, 1973 (anche in Id., *Scritti di diritto penale*, vol. I, a cura di S. Canestrari e A. Melchionda, Milano, 1997, 542 ss., p. 565).

[16] Il suo riconoscimento si deve a BINDING K., *Lehrbuch des Gemeinen Deutschen Strafrechts. Besonderer Teil*, Leipzig, 1902, p. 20 ss., il quale fu il primo ad evidenziare il «*fragmentarischen Charakters aller Strafgesetze*».

[17] Sul punto v. Corte cost., sentenza 18 luglio 1989, n. 409, che ha evidenziato come non si debbano arbitrariamente confondere «*tre distinti principi: il primo, indicato di recente da autorevole dottrina, secondo il quale non sono legittime incriminazioni penali a tutela di beni non espressivi di valori costituzionalmente rilevanti (o significativi); il secondo, enunciato come principio di proporzionalità (valido per l'intero diritto pubblico) a termini del quale la scelta dei mezzi o strumenti, da parte dello Stato, per raggiungere i propri fini "va limitata da considerazioni razionali rispetto ai valori": nel campo del diritto penale, il principio equivale a negare legittimità alle incriminazioni che, anche se presumibilmente idonee a raggiungere finalità statuali di prevenzione, producono, attraverso la pena, danni all'individuo (ai suoi diritti fondamentali) ed alla società sproporzionatamente maggiori dei vantaggi ottenuti (o da ottenere) da quest'ultima con la tutela dei beni e valori offesi dalle predette incriminazioni; ed il terzo principio, di sussidiarietà del diritto penale (quest'ultimo considerato come extrema ratio) secondo il quale è legittimo ricorrere alla sanzione penale soltanto allorché gli altri rami dell'ordinamento non offrano adeguata tutela ai beni che s'intendono garantire. I predetti principi, benché collegati (ad es. la non legittimità dell'incriminazione di fatti lesivi di beni non costituzionalmente rilevanti equivale anche a ridurre l'ambito del penalmente rilevante, come sancito dal principio di sussidiarietà) sono fra loro autonomi, indipendenti (ad es., non basta che l'incriminazione attenga ad un bene costituzionalmente rilevante per totalmente adempiere al principio di sussidiarietà, giacché, ove gli altri rami siano in grado d'offrire adeguata tutela allo stesso bene, non è legittimo che quest'ultimo sia penalmente garantito, non essendo l'incriminazione del fatto lesivo del predetto bene extrema ratio)*».

la cancellazione, il deterioramento" di cui agli artt. 4 e 5 della direttiva 2013/40/UE oppure "*l'atto di procurare per sé o per altri, compresi la ricezione, l'appropriazione, l'acquisto, il trasferimento, l'importazione, l'esportazione, la vendita, il trasporto e la distribuzione*" di cui all'art. 4 della direttiva 2019/713/UE). Con le ultime riforme, a seguito dell'implementazione degli obblighi di incriminazione di fonte sovranazionale, la punibilità è stata estesa anche al mero "possesso" di *password* o programmi informatici idonei all'accesso al sistema informatico. Il legislatore europeo, infatti, sin dalla decisione quadro 2001/413/GAI, sostituito dalla direttiva 2019/713/UE, ha obbligato gli Stati membri a punire la mera detenzione (o il possesso) di uno strumento di pagamento diverso dai contanti, che è stato rubato o altrimenti ottenuto mediante appropriazione indebita, oppure contraffatto o falsificato ai fini dell'utilizzazione fraudolenta[18]. Già la stessa Convenzione *cybercrime* aveva riconosciuto agli Stati aderenti la facoltà di punire il mero possesso di codici d'accesso, *password* e programmi informatici principalmente concepiti o destinati alla commissione di reati informatici.

1.1. La problematica dei *dual-use software*.

Le fattispecie che puniscono il possesso di dati informatici tendono a incriminare come reato a sé stante un mero atto preparatorio per il compimento di altri reati. Va, però, evidenziato che il possesso (così come le condotte di procurarsi, trasportare e simili) sono condotte "neutre" e di per sé inidonee ad offendere un bene giuridico. Il disvalore, dunque, si sposta necessariamente sulla relazione con un oggetto di per sé pericoloso (programmi informatici e altri strumenti che costituiscono oggetto materiale dei reati in esame).

Al Considerando n. 13 e 16 della direttiva 2019/713/UE il legislatore europeo ha sottolineato la necessità di evitare di criminalizzare gli strumenti di pagamento diversi dai contanti, qualora siano prodotti e posti in commercio per fini legittimi[19]. Tuttavia, come evidenziato da alcuni studiosi, non è facile individuare la corretta tecnica di tipizzazione da impiegare per selezionare in modo preciso i programmi informatici pericolosi, che possono

[18] SALVADORI I., *I reati di possesso. Un'indagine dogmatica e politico-criminale in una prospettiva storica e comparata*, Napoli, 2016, p. 34.

[19] Così il Considerando n. 16: «*la presente direttiva fa altresì riferimento a strumenti che possono essere utilizzati per commettere i reati in essa previsti. Data la necessità di evitare una criminalizzazione di tali strumenti quando essi siano prodotti e posti in commercio per fini legittimi e pertanto, anche se utilizzabili per commettere reati, non costituiscano di per sé una minaccia, la criminalizzazione dovrebbe essere limitata agli strumenti principalmente concepiti o specificamente adattati al fine di commettere i reati di cui alla presente direttiva*».

essere utilizzati per commettere reati[20]. Solo in rarissimi casi i programmi informatici vengono specificamente progettati (o possono essere utilizzati) soltanto per finalità illecite. A tal proposito, vengono denominati *dual-use software* i programmi informatici, che hanno un intrinseco carattere pericoloso, ma che possono essere utilizzati indifferentemente per finalità lecite e illecite[21] e si distinguono in *software* multifunzionali e *software* multiuso.

I *software* multifunzionali possono svolgere diverse funzioni, di cui una, però, è esclusivamente pregiudizievole ed illegittima. I *software* multiscopo, di contro, si caratterizzano per il fatto che la loro funzionalità potenzialmente dannosa o illegale, che può essere impiegata non solo per finalità illecite, ma anche per scopi del tutto leciti ed utili per la società[22]. Basti pensare a programmi quali gli *sniffer*, che monitorano, registrano e analizzano il traffico all'interno di una rete, ma che non vengono esclusivamente impiegati per commettere reati, poiché sono comunemente utilizzati per eliminare gli errori od ottimizzare il traffico di dati. È evidente che occorre evitare un'incriminazione troppo restrittiva, volta a punire i programmi esclusivamente destinati a commettere un reato. In questo caso vi sarebbe il rischio di creare disposizioni simboliche, la cui applicazione pratica sarebbe assai scarsa, se non impossibile[23].

Il legislatore europeo ha cercato di limitare l'ambito dell'oggetto materiale del reato in diversi modi. In alcuni casi ha imposto che i programmi in esame fossero «(principalmente) concepiti o adattati per commettere un reato», in altri che si trattasse di un programma «il cui scopo consista nel commettere un reato». Esempio paradigmatico del primo gruppo di disposizioni è l'art. 7 della direttiva 2013/40/UE, che obbliga gli Stati a punire condotte aventi ad oggetto un programma per computer, destinato o modificato principalmente al fine di commettere un illecito contro la riservatezza informatica, l'integrità

[20] SALVADORI I., *Criminalità informatiche e tecniche di anticipazione della tutela penale. L'incriminazione dei "dual-use software"*, in *Riv. it. dir. proc. pen.*, 2017, n. 2, p. 747 ss., p. 750.
[21] ALBRECHT M., *Die Kriminalisierung von Dual-Use-Software*, Berlin, 2014, p. 18. A tal proposito, va evidenziato che il concetto di oggetti "a duplice uso" assume una molteplicità di significati. L'art. 2 n. 1) del Regolamento 2021/821/UE del 20 maggio 2021che istituisce un regime dell'Unione di controllo delle esportazioni, dell'intermediazione, dell'assistenza tecnica, del transito e del trasferimento di prodotti a duplice uso, ad esempio, definisce i "prodotti a duplice uso" come: «*i prodotti, inclusi il software e le tecnologie, che possono avere un utilizzo sia civile sia militare e comprendono i prodotti che possono essere impiegati per la progettazione, lo sviluppo, la produzione o l'uso di armi nucleari, chimiche o biologiche o dei loro vettori, compresi tutti i prodotti che possono avere sia un utilizzo non esplosivo sia un qualsiasi impiego nella fabbricazione di armi nucleari o di altri ordigni esplosivi nucleari*».
[22] SALVADORI I., *Il diritto penale dei software "a duplice uso"* in G. Fornasari e R. Wenin (a cura di), *Diritto penale e modernità: le nuove sfide fra terrorismo, sviluppo tecnologico e garanzie fondamentali. Atti del convegno Trento 2 e 3 ottobre 2015*, Napoli, 2017, p. 361 ss., p. 373.
[23] CLOUGH J., *Principles of Cybercrime*, Cambridge, 2015, p. 135.

o la disponibilità di dati o di sistemi informatici[24]. Questa formulazione presenta un inconveniente: dato che la volontà di chi crea o adatta tali programmi informatici deve riflettersi oggettivamente nella loro struttura, la destinazione illecita dei *software* dovrà essere ricostruita sulla base della loro intrinseca configurazione. Ma in questo modo si finisce per sanzionare tutti coloro che hanno la disponibilità di uno strumento siffatto, a prescindere dalla loro effettiva intenzione di commettere o meno un illecito penale[25]. Ne conseguirebbe una dilatazione eccessiva dell'ambito applicativo delle norme incriminatrici. Insoddisfacente pare pure la scelta di selezionare soltanto programmi che oggettivamente risultino concepiti o adattati principalmente per commettere un fatto di reato. Infatti, come si è esaminato, un *software* viene normalmente progettato per diversi scopi, ma questo sarà considerato corrispondente al tipo e, quindi, illecito soltanto qualora si dimostri che la sua funzione o destinazione principale è di commettere quello specifico reato o gruppo di reati, per cui si finisce per limitare eccessivamente l'oggetto materiale del reato[26].

Per quanto riguarda il secondo gruppo di disposizioni normative in ambito europeo, sorgono difficoltà con riferimento alla definizione del concetto di "scopo". Se si ritiene che esso descriva l'obiettivo verso il quale il soggetto dirige la sua condotta, vi sarebbe il rischio di punire anche i soggetti che impieghino quel determinato programma per scopi leciti[27]. Qualora, invece, si ritenesse che lo "scopo" del *software* non coincida con l'utilizzo che ne fa il suo detentore, ma si riferisse alla sua oggettiva configurazione, si finirebbe ugualmente per dilatare eccessivamente l'ambito applicativo delle fattispecie. Ad esempio, si dovrebbero punire anche gli esperti del settore IT che impieghino un *malware* volto a realizzare un cd. *control test*. Il criterio più adeguato potrebbe pertanto essere quello di selezionare programmi informatici che si caratterizzano, su un piano oggettivo, per la loro idoneità a commettere determinati reati[28].

Come si esaminerà meglio nel prosieguo (v. infra, par. 3 e 5), a parte qualche caso sporadico (ad esempio il nuovo art. 493-*quater* c.p.) il legislatore italiano, a differenza di altri Paesi (v. *infra* cap. V, par. 2), per evitare tali inconvenienti, ha preferito incentrare il

[24] SALVADORI I., *Criminalità informatiche*, cit., p. 755 nota n. 12, il quale evidenzia che il testo italiano della direttiva, nella parte in cui descrive l'oggetto materiale del precetto, non corrisponde alle versioni in lingua straniera, poiché pone l'accento sull'intenzione di chi ha sviluppato o modificato quel determinato *software* e non sul fatto che il programma sia stato oggettivamente "concepito" o "adattato" per lo scopo.
[25] SALVADORI I., *Criminalità informatiche*, cit., p. 756.
[26] *Ibid*., p. 758.
[27] ALBRECHT M., *Die Kriminalisierung von Dual-Use-Software*, cit., p. 759.
[28] In tal senso anche SALVADORI I., *Criminalità informatiche*, cit., p. 781.

disvalore delle fattispecie sulla finalità illecita perseguita dall'autore[29]. A tal proposito è sufficiente rilevare che il reato di cui all'art. 615-*quater* c.p. non richiede alcun requisito di "adeguatezza" o "prossimità" degli atti. Ai fini della configurabilità della norma incriminatrice è sufficiente unicamente l'idoneità all'accesso dei mezzi e degli strumenti tecnici ivi elencati[30]. Tuttavia, neppure la scelta di subordinare la rilevanza penale all'esistenza di un dolo specifico appare sufficiente ad evitare la violazione del principio di proporzionalità[31]. Infatti, il mero fine criminoso non sarebbe idoneo di per sé a produrre alcuna offesa ai beni giuridici, per cui su questo non può fondare la punibilità di condotte di per sé neutre (quali il possesso o l'installazione)[32]. Né in questo caso, data la natura *dual-use*, sarebbe agevole identificare l'oggettiva idoneità della condotta a costituire il mezzo adeguato per raggiungere lo scopo perseguito.

Nelle fattispecie di cui agli artt. 615-*quater*, 615-*quinquies* e 617-*quinquies* c.p. il dolo specifico ha una funzione "differenziale": non è solo elemento costitutivo dell'illiceità penale, ma serve anche a differenziare la punibilità rispetto a fatti base identici, graduando la sanzione in base allo scopo concretamente perseguito dall'agente[33]. Le pene previste dagli artt. 615-*quater*, 615-*quinquies* c.p. e 617-*quinquies* c.p., che sono stati modificati con le novelle del 2022, variano notevolmente tra di loro, a seconda che l'installazione del programma informatico avvenga al fine di intercettare comunicazioni relative ad un sistema informatico o telematico oppure per effettuare un accesso abusivo al sistema o per danneggiarlo. Il fine che sorregge la condotta dell'agente assume un ruolo decisivo ai fini del disvalore del fatto di reato, perché con i *software* multifunzione il carattere lesivo della condotta può essere determinato sulla base dello scopo che sorregge il fatto base, di per sé "neutro". Basti pensare ad uno *sniffer*, la cui funzione consiste nell'intercettare le *password*

---

[29] Segnala SALVADORI I., *Criminalità informatiche*, cit., p. 769 s. che in qualche caso il fine descritto è addirittura legittimo: infatti, l'art. 615-*quater* c.p. punisce chiunque agisca al fine di «*procurare a sé o ad altri un profitto*»; il profitto senza la qualificazione di "ingiusto" è di per sé lecito.

[30] PICOTTI L., *Sistematica*, cit., p. 82.

[31] Così PECORELLA C., *Il diritto penale dell'informatica*, cit., p. 360. Sull'interpretazione "oggettivistica" dei reati a dolo specifico v. PICOTTI L., *Il dolo specifico. Un'indagine sugli "elementi finalistici" delle fattispecie penali*, Milano, 1993, p. 547.

[32] ANGIONI F., *Contenuto e funzioni*, cit., p. 115; MAZZACUVA N., *Il disvalore di evento nell'illecito penale. L'illecito commissivo doloso e colposo*, Milano, 1983, p. 230; SALVADORI I., *I reati di* possesso, cit., p. 270. A tal proposito BRICOLA F., *Teoria generale del reato*, cit., p. 789 sosteneva che «*non sono costituzionalmente legittime fattispecie criminose in cui un particolare dolo specifico, espressione di una direzione lesiva, si radichi su di una condotta "neutrale", ossia di per sé non offensiva di un valore costituzionalmente significativo. In tali casi tutto il fuoco del disvalore si incentrerebbe su di un mero atteggiamento psichico: la differenza che corre tra queste ipotesi e la repressione penale della* Gesinnung *è assai tenue*».

[33] PICOTTI L., *Il dolo specifico*, cit., p. 80 ss.; MAZZACUVA N., *Il disvalore di evento nell'illecito penale*, cit., p. 221.

o i dati che vengono inseriti in un sistema informatico: esso è idoneo non solo ad intercettare le comunicazioni tra sistemi, ma anche a favorire un successivo accesso abusivo al sistema informatico. È evidente che un programma informatico di questo tipo non è specificamente destinato a realizzare una sola delle finalità criminose richiamate dalle norme incriminatrici in esame, potendo avere, come si è detto, molteplici funzioni. Di conseguenza, il trattamento sanzionatorio varia in relazione allo scopo per il quale il programma in questione viene utilizzato. Nella pratica, però, appare difficile distinguere quando l'installazione del programma informatico sia avvenuto al fine di intercettare comunicazioni relative ad un sistema informatico o telematico, per effettuare un successivo accesso abusivo al sistema oppure allo scopo di danneggiarlo.

La ragione per la quale è stata operata la scelta di punire meri atti preparatori pare risiedere nell'esigenza di facilitare le indagini delle forze di Polizia, consentendo l'intervento anticipatamente, così da scongiurare la commissione di più gravi reati informatici[34]. L'esigenza di contrastare fenomeni criminosi che effettivamente hanno assunto una portata preoccupante non può, tuttavia, comportare il sacrificio dei fondamentali principi del diritto penale[35].

È indubbio che molti *malware* siano oggettivamente pericolosi, se utilizzati per attaccare le infrastrutture critiche, il cui regolare funzionamento dipende dalla integrità e disponibilità di dati e di sistemi informatici che le gestiscono. Il ricorso allo strumento penale per punire le condotte di installazione o di compravendita aventi ad oggetto i *malware* appare dunque necessario. Appare scelta più adeguata focalizzare il disvalore del reato sulle condotte e selezionare quelle che davvero sono meritevoli di considerazione penale, eliminando tutte le altre, a partire dal mero possesso. Questa scelta verrebbe però a contrapporsi a quanto stabilito dal legislatore europeo, con le direttive 2013/40/UE e 2019/713/UE, le quali impongono agli Stati membri di sanzionare un ampio ventaglio di condotte. Come si può desumere da un'importante sentenza della Corte costituzionale[36], l'impegno assunto dal nostro Paese in sede europea di punire anche la semplice detenzione o il possesso di determinati oggetti (materiali o immateriali) non può travolgere i principi–cardine del nostro ordinamento penale. Ma, a monte, dovrebbe essere compito del legislatore

[34] FUMO M., *La condotta nei reati informatici*, in *Arch. pen.*, 2013, p. 771 ss., p. 781 s.
[35] *Ibid.*, p. 783.
[36] Cft. Corte cost., sentenza 31 maggio 2018, n. 115, di conclusione della c.d. "saga Taricco", la quale ha ribadito che il primato del diritto dell'Unione quale dato acquisito nella giurisprudenza costituzionale, ai sensi dell'art. 11 Cost., è condizionato all'osservanza dei "principi supremi dell'ordine costituzionale italiano e dei diritti inalienabili della persona".

europeo cercare di razionalizzare e armonizzare il sistema vigente, muovendo da una chiara individuazione dei beni ed interessi meritevoli e bisognosi di specifica protezione penale, selezionando tecniche di incriminazione rispettose delle esigenze di tassatività, offensività, *extrema ratio* e proporzionalità[37]. Finora questo non è sempre stato garantito, favorendo, in specie nell'ambito della criminalità informatica, una moltiplicazione di fattispecie penali, la cui formulazione non sempre è rispettosa dei principi penalistici.

2. Il reato di accesso abusivo ad un sistema informatico o telematico di cui all'art. 615-*ter* c.p.

Tra le fattispecie di più frequente applicazione vi è sicuramente il reato di accesso abusivo a sistema informatico o telematico. Si tratta di un reato prodromico alla commissione di ulteriori reati. Infatti, a parte l'ipotesi limite in cui venga commesso per mero divertimento, è di regola strumentale all'ulteriore realizzazione di un comportamento illecito, quale, ad esempio, l'acquisizione di dati e programmi altrimenti non disponibili o, comunque, non disponibili a quelle condizioni[38].

La formulazione dell'art. 615-*ter* c.p. ricalca quella del reato tradizionale di violazione di domicilio. Esso punisce sia colui che si introduca abusivamente in un sistema informatico, sia colui che "vi si mantenga" contro la volontà espressa o tacita di chi ha diritto di escluderlo. Evidente è, dunque, il richiamo alla condotta del trattenersi di cui all'art. 614, co. 2, c.p.[39]. Si differenzia, però, da quest'ultima fattispecie perché il bene giuridico tutelato è un bene giuridico nuovo, che va oltre la sfera delle informazioni che riguardano determinate persone fisiche o il domicilio come luogo, o l'ambito dei segreti[40]. In realtà, l'individuazione del bene giuridico tutelato dalla norma in esame è dibattuta. Per la sua collocazione nella sezione dedicata ai reati contro l'inviolabilità del domicilio, alcuni autori hanno ritenuto che il bene giuridico tutelato dalla norma sia il domicilio informatico[41]. Per

[37] PICOTTI L., *Nuove tecnologie e beni giuridici della persona*, cit., p. 75.
[38] PECORELLA C., *Il diritto penale dell'informatica*, cit., p. 312.
[39] SALVADORI I., *I reati contro la riservatezza informatica*, cit., p. 667.
[40] PICOTTI L., *Sistematica*, cit., p. 78, secondo cui: «*essa riguarda il "nuovo interesse all'esclusività (o possibilità autonoma di controllo e limitazione) dell'accesso, utilizzo, trattamento di dati e sistemi informatici in quanto tali, che si giustifica per la (ben maggiore) utilità così garantita al titolare di fronte all'altrimenti "strutturale" accessibilità, facilità di circolazione ed ampiezza di diffusione – proprio attraverso le connessioni e procedure automatizzate – dei dati e delle informazioni*».
[41] In tal senso v. PICA G., *Diritto penale delle tecnologie informatiche*, cit., p. 68; FUMO M., *La condotta nei reati informatici*, cit., p. 773 s.; CUOMO L., *La tutela penale del domicilio informatico*, in *Cass. pen*., 2000, n. 11, p. 2998 ss., p. 2998; ALMA M.M., PERRONI C., *Riflessioni sull'attuazione delle norme a tutela dei sistemi informatici*, in *Dir. pen. e processo*, 1997, n. 4, p. 504 ss., p. 505; GALDIERI P., *La tutela penale del domicilio informatico*, in ID. (a cura di), *Problemi giuridici dell'informatica nel MEC*, Milano, 1996, p. 189 ss. Questa, peraltro, era anche l'opinione del legislatore del 1993, il quale nella *Presentazione del Ministro di*

altri, invece, esso andrebbe individuato nell'integrità del sistema informatico[42]. Nessuna di tali tesi, però, appare persuasiva. La prima non appare idonea a cogliere le peculiarità degli spazi virtuali; la seconda, di contro, perché finisce per sovrapporre piani distinti, anche se strettamente correlati. Più corretta pare la tesi che identifica il bene giuridico protetto dalla norma in questione nella riservatezza informatica[43].

Oggetto materiale del reato è un sistema informatico o telematico protetto da misure di sicurezza. Dottrina e giurisprudenza accolgono un'interpretazione lata di sistema informatico, quale complesso di raccolta ed elaborazione di dati, composto sia da elementi di *hardware* che da elementi di *software*[44]. Costituisce, dunque, sistema informatico sia la "macchina" nel suo insieme, che la somma delle sue componenti[45]. La Suprema Corte ha qualificato come "sistema informatico", oltre al singolo computer[46], anche il sistema di pagamento POS[47] e la rete telefonica[48]. Si è evidenziato che nelle linee telefoniche moderne la funzione di trasmissione delle comunicazioni si attua con la conversione (codificazione) dei segnali (nel caso fonici) in forma di flusso continuo di cifre (*bit*) e nel loro trasporto in tale forma all'altro estremo, dove il segnale di origine viene ricostruito (decodificazione) e inoltrato, dopo essere stato registrato in apposite memorie. Pertanto, il centralino e le reti telefoniche sono qualificabili come sistemi informatici non solo perché abilitano le linee alla chiamata di determinate utenze e non di altre, ma anche per la possibilità di memorizzare e trattare elettronicamente le informazioni relative ai "dati esterni alle conversazioni", come il numero dell'abbonato chiamante, dell'abbonato chiamato, il totale degli scatti, la data e l'ora della conversazione, che possono essere stampati su appositi tabulati contenenti il flusso di

---

Grazia e Giustizia (v. nota 4), ha evidenziato che «*la normativa trova la sua collocazione tra i reati contro l'inviolabilità del domicilio perché i sistemi informatici o telematici, la cui violazione essa reprime, costituiscono un'espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantito dall'art. 14 della Costituzione e penalmente tutelata nei suoi aspetti più essenziali e tradizionali dagli articoli 614 e 615 del codice penale*».

[42] PARODI C., *I reati patrimoniali*, in C. Parodi, V. Sellaroli (a cura di), *Diritto penale dell'informatica. Reati della rete e sulla rete*, Milano, 2020, p. 103 ss., p. 129.

[43] PICOTTI L., *Sistematica*, cit., p. 78; SALVADORI I., *I reati contro la riservatezza informatica*, cit., p. 667.

[44] GATTA G.L., *Delitti contro l'inviolabilità del domicilio*, in F. Viganò, C. Piergallini (a cura di), *Reati contro la persona e contro il patrimonio*, in *Trattato teorico/ pratico di diritto penale*, diretto da Palazzo F. e Paliero C.E., II ed., Torino, 2015, p. 317 ss., p. 334.

[45] La Convenzione *Cybercrime* di Budapest all'art. 1, lett. a), definisce "sistema informatico" come «*qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione automatica di dati*».

[46] CORRIAS LUCENTE G., *Brevi note in tema di accesso abusivo e frode informatica: uno strumento per la tutela penale dei servizi*, in *Dir. inf. inf*., 2001, n. 3, p. 492 ss., p. 495, la quale ha evidenziato che «*da una prospettiva di politica criminale, del resto, sarebbe paradossale espungere i personal computers dall'orbita di tutela, atteso che le medesime esigenze poste a fondamento della fattispecie di accesso abusivo sono correlate al loro impiego*».

[47] Cass. pen., sez. fer., sentenza 23 agosto 2012, n. 43755.

[48] Cass. pen., sez. VI, sentenza 4 ottobre 1999, n. 3065.

comunicazioni informatiche o telematiche[49].

Sistema telematico è, invece, un insieme combinato di apparecchiature idoneo alla trasmissione di dati e informazioni attraverso l'impiego di tecnologie dedicate alle telecomunicazioni[50].

L'art. 615-*ter* c.p. si configura come un reato di mera condotta e si consuma con l'accesso al sistema informatico protetto, senza che sia necessario che l'intrusione sia effettuata allo scopo di violare la riservatezza degli utenti ovvero con la "permanenza" nel suddetto sistema[51]. In passato si è creato un contrasto giurisprudenziale, relativo all'individuazione *locus commissi delicti* e, di conseguenza, della competenza territoriale con riferimento al reato in esame. Sul punto sono intervenute le Sezioni Unite della Corte di Cassazione, le quali hanno accolto l'orientamento secondo cui il luogo di consumazione del delitto di accesso abusivo ad un sistema informatico o telematico è quello nel quale si trova il soggetto che effettua l'introduzione abusiva o vi si mantiene abusivamente, non quello ove sono collocati il *Server* o la banca dati che elaborano e controllano le credenziali di autenticazione del *client*[52].

La Suprema Corte, nello specifico, ha evidenziato che la nozione di collocazione spaziale o fisica è essenzialmente estranea alla circolazione dei dati. Questi ultimi, infatti, se archiviati su *cloud computing* o comunque resi disponibili dal *Server* che sfruttano tali servizi, sono collocati su piattaforme accessibili a livello globale. Diventa pertanto difficile individuare il luogo esatto nel quale le informazioni sono collocate. La Suprema Corte ha respinto la tesi secondo la quale il reato di accesso abusivo si consuma nel luogo in cui è collocato il *Server* che controlla le credenziali di autenticazione del *client* non potesse essere condivisa, in quanto, in ambito informatico, deve attribuirsi rilevanza, più che al luogo in cui materialmente si trova il sistema informatico, a quello da cui parte il dialogo elettronico tra i sistemi interconnessi e dove le informazioni vengono trattate dall'utente. Il luogo di consumazione s'identifica con quello nel quale dalla postazione remota l'agente s'interfaccia con l'intero sistema, digita le credenziali di autenticazione e preme il tasto di avvio, ponendo

---

[49] *Ibid*.
[50] CUOMO L., *La tutela penale del domicilio informatico*, cit., p. 2999.
[51] PARODI C., *I reati patrimoniali*, cit., p. 129; in giurisprudenza v. Cass. pen., sez. V, sentenza 20 marzo 2007, n. 11689 e Cass. pen., sez. I, sentenza 27 settembre 2013, n. 40303, secondo cui: «*l'accesso o il mantenimento abusivi sono puniti, dunque, in quanto tali non rilevando lo scopo perseguito dall'utente che rimane un fatto ultroneo rispetto alla condotta punibile, potendo, infatti, il client abusivo aver voluto violare il sistema per mero atto dimostrativo, ma anche per danneggiare il sistema, ovvero per accedere a informazioni riservate onde apprenderle per le ragioni più svariate. Da qui la natura eventualmente strumentale dell'accesso abusivo che ben può concorrere con altri delitti, informatici e non*».
[52] Cass. pen., sez. un., sentenza 26 marzo 2015, n. 17325.

così in essere l'unica azione materiale e volontaria. Lo stesso dicasi per l'ipotesi omissiva di mantenimento abusivo: anche in questo caso il reato si consuma nel luogo in cui l'utente è rimasto connesso al sistema[53].

Le condotte penalmente rilevanti consistono nell'introdursi abusivamente in un sistema informatico protetto e nel mantenersi in esso contro la volontà di chi ha diritto di escluderlo. L'utilizzo del termine "introdursi" in luogo di quello di "accesso", utilizzato da altri legislatori europei, è stato criticato da una parte della dottrina[54]. Si è infatti osservato che l'utilizzo di tale termine appare più appropriato per individuare condotte che consistono nel varcare spazi fisicamente delimitati, che, però, non sono identificabili nel caso del sistema informatico o telematico. In ogni caso, si ritiene che l'intrusione debba essere intesa in senso ampio, così da abbracciare non solo l'accesso c.d. fisico ottenuto attraverso il contatto diretto col computer, ma anche quello "logico", compiuto attraverso le reti telematiche[55]. Al fine di non dilatare eccessivamente l'ambito applicativo della fattispecie, si richiede che l'intrusione penalmente rilevante non possa consistere semplicemente nell' "entrare in contatto" con il sistema informatico o telematico. Se così fosse il reato in esame si configurerebbe anche nell'ipotesi di un mero contatto fisico con il computer. Si ritiene, invece, necessaria l'instaurazione di un dialogo logico o automatizzato con la sua parte *software*[56]. In tal senso l'accesso si configurerebbe unicamente nel momento in cui il sistema informatico altrui esegua una data operazione a seguito dell'impulso dato dai comandi del soggetto agente, il quale viene così messo nelle condizioni di poter operare nel sistema e conoscerne il contenuto[57].

---

[53] In dottrina è favorevole a tale tesi BELLACOSA M., *Il luogo di consumazione del delitto di accesso abusivo a un sistema informatico o telematico: in attesa delle Sezioni Unite*, in *Dir. Pen. Cont*., 2 febbraio 2015, p. 1 ss. Diversamente FLOR R., *I limiti del principio di territorialità nel cyberspace. Rilievi critici alla luce del recente orientamento delle Sezioni Unite*, in *Dir. pen. proc*., 2015, n. 10, p. 1291 ss., p. 1301 ss., evidenzia come la soluzione prospettata dalle Sezioni Unite possa adattarsi unicamente all'accesso del c.d. *insider*, perché in tutti gli altri casi l'accesso a spazi informatici non sempre avviene in luoghi fisicamente e territorialmente individuabili. Inoltre, tale soluzione mal si adatta alla diversa condotta del mantenimento, in quanto esso si consuma nel momento della contravvenzione alle disposizioni predisposte dal titolare, a prescindere dalle successive attività che ne conseguano causalmente o dalle finalità perseguite dal soggetto attivo.

[54] SALVADORI I., *L'accesso abusivo ad un sistema informatico*, cit., p. 134.

[55] MUCCIARELLI F., *Commento all'art. 4 della legge 23 dicembre 1993 n. 547 - Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica*, in *Leg. pen*., 1996, n. 1-2, p. 99 ss., p. 99; PICA G., *Diritto penale delle tecnologie informatiche*, cit., p. 41; SALVADORI I., *L'accesso abusivo ad un sistema informatico*, cit., p. 135.

[56] PERRI P., *Analisi informatico-giuridica dei reati di frode informatica e accesso abusivo ad un sistema informatico o telematico con l'aggravante dell'abuso della qualità di operatore del sistema*, in *Giur. Merito*, 2008, n. 6, p. 1651 ss., p. 1656; SALVADORI I., *I reati contro la riservatezza informatica*, cit., p. 668.

[57] V. Cass. pen., sez. V, sentenza 8 luglio 2008, n. 37322, secondo cui «*per accesso - così la rubrica dell'art. 615 ter c.p. - deve ritenersi, come chiarito da autorevole dottrina, non tanto il semplice collegamento fisico, ovvero l'accensione dello schermo ecc., ma quello logico, ovvero il superamento della barriera di protezione del sistema, che renda possibile il dialogo con il medesimo in modo che l'agente venga a trovarsi nella*

La norma punisce l'accesso non autorizzato ad un sistema informatico e non richiede che il soggetto agente acceda ai dati o ai programmi in esso contenuti. Pertanto, ai fini dell'integrazione della condotta tipica, è irrilevante che il reo abbia preso cognizione del loro contenuto[58]. Il reato in esame integra un'ipotesi di reato di pericolo astratto, dato che la tutela del bene giuridico della riservatezza informatica viene anticipata ad una fase anteriore all'effettiva acquisizione e sottrazione di dati e informazioni[59]. Secondo un diverso orientamento, però, l'art. 615-*ter* c.p. integrerebbe un reato di danno, dato che la fattispecie in realtà non si consumerebbe con il mero accesso, ma con la effettiva presa di coscienza o sottrazione dei dati ivi contenuti[60]. Tale ultima interpretazione, però, non sembra condivisibile, in quanto contrasta col tenore letterale della norma.

Oltre alla condotta di introduzione, l'art. 615-*ter* c.p. sanziona anche quella del mantenimento nel sistema predetto contro la volontà espressa o tacita di chi ha diritto di escluderlo, alternativa rispetto a quella dell'introduzione[61]. La natura di tale condotta è controversa: per alcuni autori si tratterebbe di condotta omissiva[62], mentre per altri costituirebbe un'ipotesi commissiva[63]. La prima interpretazione è più condivisibile, dato che, come evidenziato in precedenza, l'art. 615-*ter* c.p. è formulato prendendo come modello il reato di violazione di domicilio.

Il mantenimento consente di punire i casi di volontaria permanenza, a seguito di un legittimo accesso, in uno spazio virtuale, nonostante la contraria volontà del titolare, che non

---

condizione di conoscere dati, informazioni e programmi; la conoscenza dei dati, evidentemente, può avvenire sia con la semplice lettura, sia con la copiatura degli stessi». Nello stesso senso anche Cass. pen., sez. I, sentenza 27 settembre 2013, n. 40303.

[58] SALVADORI I., *I reati contro la riservatezza informatica*, cit., p. 668; PECORELLA C., *Il diritto penale dell'informatica*, cit., p. 336. *Contra* D'ARCANGELO F., *L'accesso abusivo ad un sistema informatico nell'era di Internet*, in *Corr. mer.*, 2008, n. 10, p. 1066 ss., p. 1074; MANTOVANI F., *Diritto penale, PS, I delitti contro la persona*, vol. I, VI ed., Padova, 2016, p. 575; NUNZIATA M., *La prima applicazione giurisprudenziale del delitto di "accesso abusivo ad un sistema informatico" ex art. 615 ter c.p.*, in *Giur. Mer.*, n.4-5, 1998, p. 708 ss., p. 715, i quali, invece, ritengono che il delitto di cui all'art. 615-*ter* c.p. non sia integrato con la mera introduzione nell'altrui sistema informatico, ma sostengono sia necessario un accesso, almeno potenziale, alla conoscenza dei dati o delle informazioni contenute nello stesso.

[59] CUOMO L., *La tutela penale del domicilio informatico*, cit., p. 3000; FLOR R., *sub art. 615-ter c.p.*, in G. Forti, S. Seminara, G. Zuccalà (a cura di), *Commentario breve al Codice Penale*, VI ed., Padova, 2017, p. 2129 ss., p. 2130.

[60] In tal senso BERGHELLA F., BLAIOTTA R., *Diritto penale dell'informatica e beni giuridici*, cit., p. 2333, secondo cui «*ragioni afferenti alla complessiva strategia della legge sconsigliano di configurare il reato in esame come illecito di pericolo*», nonché ATERNO S., *Sull'accesso abusivo a un sistema informatico o telematico*, in *Cass. pen.*, 2000, n. 11, p. 2994 ss., p. 2996.

[61] NUNZIATA M., *La prima applicazione giurisprudenziale*, cit., p. 715.

[62] PICOTTI L. voce *Reati informatici*, cit., p. 22; SALVADORI I., *L'accesso abusivo ad un sistema informatico*, cit., p. 137; MUCCIARELLI F., *Commento all'art. 4*, cit., p. 100.

[63] FLOR R., *Art. 615 ter c.p.: natura e funzioni delle misure di sicurezza, consumazione del reato e bene giuridico protetto*, in *Dir. pen. proc.*, 2008, n. 1, p. 106 ss., p. 111; PICA G., *Diritto penale delle tecnologie informatiche*, cit., p. 41.

sarebbero altrimenti sussumibili nella diversa condotta di intrusione[64].

La permanenza non può essere intesa in senso fisico, ma come mantenimento della connessione logica al sistema informatico o telematico[65]. Dalla norma appare evidente che il legislatore del 1993 ha inteso punire la mera permanenza nel sistema e non le attività contestualmente compiute in relazione a tale accesso. Pertanto, pare corretto ritenere per cui si concorda con coloro che ritengono priva di rilevanza ai fini della consumazione dell'illecito in questione l'effettiva presa di conoscenza di dati o informazioni[66].

Le condotte di "intrusione" e permanenza devono essere compiute "abusivamente". In realtà, per quanto riguarda la permanenza, la norma richiede che essa avvenga «*contro la volontà espressa o tacita di chi ha diritto di escluderlo*». Non si ritiene, tuttavia, che tale locuzione sia idonea a connotare il fatto di un diverso disvalore lesivo, trattandosi di mera scelta stilistica[67]. Per qualche autore si tratterebbe di un'indicazione meramente pleonastica, che non fa altro che sottolineare la necessaria antigiuridicità del fatto di reato[68]. Un diverso orientamento condivisibilmente ritiene che la stessa abbia, al pari dell'avverbio "abusivamente", un ruolo essenziale all'interno della fattispecie in quanto requisito di illiceità speciale, evidenziando che le condotte di introduzione e di mantenimento in un sistema informatico protetto diventano penalmente rilevanti qualora siano poste in essere senza autorizzazione[69]. L'abusività delle condotte di introduzione o di permanenza viene oggi determinata sulla base di una manifestazione di contrarietà (espressa o tacita) da parte del titolare o dell'amministratore del sistema[70]. Si ritiene, però, preferibile, intendere l'abusività non solo come mancanza di autorizzazione, ma anche come violazione dei limiti della stessa[71], dato che la norma incriminatrice fa riferimento anche alla mancanza del consenso da parte del titolare del sistema.

Il carattere abusivo della condotta acquista notevole importanza nell'economia

---

[64] PICA G., *Diritto penale delle tecnologie informatiche*, cit., p. 42; PECORELLA C., *Il diritto penale dell'informatica*, cit., p. 351.
[65] SALVADORI I., *I reati contro la riservatezza informatica*, cit., p. 669.
[66] FLOR R., *Verso una rivalutazione dell'art. 615 ter c.p.? Il reato di accesso abusivo a sistemi informatici o telematici fra la tutela di tradizionali e di nuovi diritti fondamentali nell'era di Internet*, in *Riv. trim. dir. pen. cont*., 2012, n. 2, p. 126 ss., p. 131; SALVADORI I., *I reati contro la riservatezza informatica*, cit., p. 669.
[67] SALVADORI I., *I reati contro la riservatezza informatica*, cit., p. 670.
[68] PAZIENZA F., *In tema di criminalità informatica: l'art. 4 della legge 23 dicembre 1993*, n. 547, in *Riv. it. dir. proc. pen*., 1995, n. 3, p. 750 ss., p. 756.
[69] FLOR R., *Verso una rivalutazione dell'art. 615 ter c.p.?*, cit., p. 132; SALVADORI I., *I reati contro la riservatezza informatica*, cit., p. 670 s., il quale evidenzia che «*se tale requisito venisse soppresso, la previsione legale non avrebbe alcun senso, dato che le condotte di introduzione e di permanenza in un sistema informatico o telematico sono di per sé prive di autonoma carica offensiva*».
[70] PICA G., *op. cit*., p. 51 s.; GATTA G.L., *Delitti contro l'inviolabilità del domicilio*, cit., p. 353 s.; FLOR R., *Verso una rivalutazione dell'art. 615 ter c.p.?*, cit., p. 132.
[71] Così anche SALVADORI I., *I reati contro la riservatezza informatica*, cit., p. 671.

dell'art. 615-*ter* c.p., in particolare per quanto riguarda la condotta del c.d. *insider*, qualora, essendo in possesso delle credenziali di accesso, acceda al sistema per una finalità diversa rispetto a quella consentita. Sul punto si sono contrapposte due tesi. Per un primo orientamento, penalmente rilevante potrebbe considerarsi solo l'accesso abusivo, effettuato da un soggetto non abilitato. Contrariamente, sarebbe sempre lecito l'accesso del soggetto autorizzato, ancorché venisse effettuato per finalità estranee a quelle d'ufficio ovvero illecite. Alla base di tale tesi vi è l'idea che la volontà contraria del titolare del sistema, e la conseguente qualificazione in termini di abusività della condotta posta in essere dall'agente, debbano essere verificate esclusivamente con riguardo al momento dell'accesso al sistema informatico o telematico o del mantenimento al suo interno e non già con riferimento ai fatti criminosi successivi che l'agente abbia intenzione di porre in essere, poiché questi ultimi potrebbero acquisire rilevanza solo in conseguenza di nuove e diverse determinazioni volitive ed a seconda degli specifici connotati che le ulteriori condotte avessero assunto in concreto una volta poste in essere. La qualificazione di abusività sarebbe, in definitiva, da intendersi in senso oggettivo, con riferimento al momento dell'accesso e alle modalità utilizzate dall'autore per superare le misure di sicurezza apprestate dal titolare[72].

Per il secondo indirizzo, andrebbe considerata abusiva l'utilizzazione dell'autorizzazione per uno scopo diverso rispetto a quello per la quale è stata conferita. Pertanto, nel momento in cui l'agente autorizzato ad accedere al sistema impiegare il titolo di legittimazione per conseguire una finalità illecita, o comunque diversa rispetto a quella per la quale l'accesso era stato concesso, tale condotta, poiché in contrasto con la *voluntas domini*, diventerebbe abusiva[73]. Anche secondo tale filone interpretativo la norma in esame punirebbe non solo la condotta di abusiva "introduzione", ma anche quella d'illecito trattenimento all'interno del sistema. Di conseguenza, si configurerebbe un'ipotesi di mantenimento all'interno del sistema contro la volontà tacita del titolare dello *ius excludendi*, poiché l'accesso da parte del soggetto abilitato, di per sé legittimo, diverrebbe abusivo e perciò illecito qualora l'agente permanesse all'interno del sistema per fini e ragioni estranee

[72] PECORELLA C., *L'attesa pronuncia delle Sezioni Unite sull'accesso abusivo a un sistema informatico: un passo avanti non risolutivo*, in *Cass. pen.*, 2012, n. 11, p. 3692 ss., p. 3703 s.; MENGONI E., *Accesso autorizzato al sistema informatico o telematico e finalità illecite: nuovo round alla configurabilità del reato*, in *Cass. pen.*, 2011, n. 6, p. 2200 ss., p. 2205 s.; CIVARDI S., *La distinzione fra accesso abusivo a sistema informatico e abuso dei dati acquisiti*, in *Dir. inf. inf.*, 2009, n. 1, p. 58 ss., p. 63; FLOR R., *Permanenza non autorizzata in un sistema informatico o telematico, violazione del segreto d'ufficio e concorso nel reato da parte dell'extraneus*, in *Cass. pen.*, 2009, n. 4, p. 1509 ss., p. 1513; SALVADORI I., *I reati contro la riservatezza informatica*, cit., p. 675.

[73] DE FLAMMINEIS S., *Art. 615-ter c.p.: accesso legittimo ma per finalità estranee ad un sistema informatico*, in *Cass. pen.*, 2011, n. 6, p. 2209 ss., p. 2211 ss.

a quelle legittime[74].

La questione è dibattuta anche in giurisprudenza. Inizialmente le Sezioni Unite avevano escluso che integrasse il reato di cui all'art. 615-*ter* c.p. la condotta di accesso o di mantenimento nel sistema da parte di soggetto abilitato all'accesso, ma attuata per scopi o finalità estranei a quelli per i quali tale facoltà gli era stata attribuita. In particolare, i giudici avevano sostenuto non si dovesse guardare alle finalità perseguite da colui che accede o si mantiene nel sistema, poiché la volontà del titolare del diritto di escluderlo si connoterebbe soltanto per il dato oggettivo della permanenza dell'agente. La contraria volontà del titolare del sistema andrebbe così verificata solo con riferimento al risultato immediato della condotta posta in essere, non già alla luce dei fatti successivi[75]. In principio, dunque, la Corte ha sancito l'irrilevanza della finalità perseguita dal soggetto agente. Tuttavia, i giudici di legittimità hanno evidenziato che l'accesso al sistema è abusivo non soltanto qualora avvenga "senza autorizzazione", ma anche eccedendone i limiti[76]. Di conseguenza, la permanenza nel sistema informatico andrebbe intesa come abusiva qualora il soggetto continuerebbe ad accedere alla "conoscenza dei dati" nonostante il venir meno dell'autorizzazione da parte del titolare dello *jus excludendi alios*.

La giurisprudenza successiva non ha accolto favorevolmente tale soluzione, per cui il nodo interpretativo è stato nuovamente rimesso alle Sezioni Unite[77]. La Corte di Cassazione, pronunciandosi in merito all'accesso al sistema informatico compiuto dal pubblico ufficiale per finalità extraistituzionali, ha aderito all'orientamento contrario. Nello specifico, ha ritenuto che la condotta del pubblico ufficiale o dell'incaricato di un pubblico servizio che, pur essendo abilitato e senza violare le prescrizioni formali impartite dal titolare di un sistema informatico o telematico protetto per delimitare l'accesso, vi acceda o si intrattenga per ragioni ontologicamente e comunque diverse rispetto a quelle per le quali soltanto la facoltà di accesso gli è attribuita, integri il delitto previsto dall'art. 615-*ter*, co. 2, n. 1, c.p.[78]. Le Sezioni Unite hanno dunque ritenuto rilevanti le finalità per le quali l'accesso viene effettuato. Qualora esso avvenga per scopo estraneo alle mansioni configura sviamento

[74] In tal senso v. Cass. pen., sez. V, sentenza 7 novembre 2000 n. 12732; Cass. pen., sez. V, sentenza 8 luglio 2008 n. 37322; Cass. pen., sez. V, sentenza 16 gennaio 2009, n. 1727; Cass. pen., sez. V, sentenza 30 aprile 2009, n. 18006; Cass. pen., sez. V, sentenza 22 gennaio 2010, n. 2987; Cass. pen., sez. V, sentenza 21 maggio 2010 n. 19463; Cass. pen., sez. IV, sentenza 20 giugno 2011 n. 24583.
[75] Cass. pen., sez. un., sentenza 7 febbraio 2012, n. 4694.
[76] A tal proposito SALVADORI I., *Quando un* insider *accede abusivamente ad un sistema informatico o telematico? Le Sezioni Unite precisano l'ambito di applicazione dell'art. 615-ter c.p.*, in *Riv. trim. dir. pen. econ.*, 2012, n. 1-2, p. 369 ss., p. 374, il quale ha sollevato dubbi in merito alla compatibilità dell'interpretazione estensiva dell'avverbio "abusivamente" col divieto di analogia *in malam partem*.
[77] V. Cass. pen., sez. V, ordinanza 25 gennaio 2017, n. 12264.
[78] Cass. pen., sez. un., sentenza 8 settembre 2017, n. 41210.

di potere, non si può che stigmatizzare negativamente la condotta, dato che la legittima "fruizione" di un sistema informatico viene illegittimamente destinata al soddisfacimento di un interesse personale e privato. Il contrasto interpretativo rimane pertanto aperto.

L'art. 615-*ter* c.p. richiede poi che il sistema informatico violato sia protetto da misure di sicurezza. Non è, invece richiesta la loro violazione[79]. Il concetto di misure di sicurezza dev'essere inteso in senso lato. Esso abbraccia sia di misure di carattere logico (quale ad esempio una *password*), sia fisico (ad esempio un *token*)[80]. In ogni caso, è necessario che le stesse costituiscano un ostacolo serio e concretamente difficile da superare[81]. Non si ritiene, però, che le impostazioni di sicurezza di un *browser*, definite dal produttore per la navigazione sul *web*, possano rientrare nella nozione di misura di sicurezza. Se così fosse si dilaterebbe in modo eccessivo l'ambito applicativo della norma in questione[82].

L'elemento soggettivo è costituito dal dolo generico, nel cui fuoco devono rientrare tutti gli elementi costitutivi della fattispecie, così come la consapevolezza che il sistema violato è protetto da misure di sicurezza[83].

L'art. 615-*ter* c.p. prevede diverse circostanze aggravanti ad effetto speciale, che comportano anche la procedibilità d'ufficio del reato. La prima, di cui all'art. 615-*ter*, co. 2, n. 1, c.p. è un'aggravante soggettiva[84], che si applica qualora il fatto sia commesso da un pubblico ufficiale, da un incaricato di pubblico servizio, con abuso dei relativi poteri o violazione dei doveri su di essi incombenti, ovvero da chi eserciti, ancorché abusivamente,

---

[79] SALVADORI I., *L'accesso abusivo ad un sistema informatico*, cit., p. 143.

[80] Così PARODI C., CALICE A., *Responsabilità penali e Internet. Le ipotesi di responsabilità penale nell'uso dell'informatica e della telematica*, Milano, 2001, p. 64; PICA G., *Diritto penale*, cit., p. 53; SALVADORI I., *L'accesso abusivo ad un sistema informatico*, cit., p. 144. È rimasta isolata, invece, la tesi di CECCACCI G., *Computer Crimes. La nuova disciplina sui reati informatici*, Milano, 1994, p. 70 ss., secondo cui le misure di sicurezza di cui all'art. 615-*ter* c.p. non si esaurirebbero in una semplice *password*, ma dovrebbero necessariamente garantire un certo grado di sicurezza, complessità ed affidabilità.

[81] SPAGNOLETTI V., *Art. 615 ter c.p.: il domicilio informatico tra profili dogmatici e problemi applicativi*, in *Giur. mer.*, 2004, n. 1, p. 181 ss., p. 183.

[82] Così anche SALVADORI I., *L'accesso abusivo ad un sistema informatico*, cit., p. 145, il quale evidenzia che «*questa interpretazione lata del concetto di misure di sicurezza svuoterebbe però il significato politico-criminale del requisito della protezione dei sistemi, richiesto dalla fattispecie di accesso abusivo, portando a ritenere che, nell'attuale prevalenza di una monocultura informatica, tutti i sistemi informatici dotati di un sistema operativo della Microsoft siano di fatto "protetti" da misure di sicurezza*».

[83] FLOR R., sub *art. 615-ter c.p.*, cit., p. 2131.

[84] In tal senso Cass. pen., sez. un., sentenza 8 settembre 2017, n. 41210, cit. Secondo FLOR R., *La condotta del pubblico ufficiale fra violazione della* voluntas domini*, "abuso" dei profili autorizzativi e "sviamento di potere"*, in *Dir. pen. proc.*, 2018, n. 4, p. 506 ss., p. 514, sebbene le Sezioni Unite parlino di circostanza aggravante, in realtà la qualificano come un'ipotesi autonoma di reato, in particolare quando affermano che il pubblico ufficiale e l'incaricato di pubblico servizio «*possono rispondere del reato solo in forza della previsione del co. 2*» e che per «*tali soggetti il reato è sempre aggravato proprio perché legato alla qualità soggettiva*».

la professione di investigatore privato, ovvero con abuso della qualità di "operatore di sistema".

Per quanto riguarda la qualifica di pubblico ufficiale o incaricato di pubblico servizio, la giurisprudenza ha specificato che ai fini dell'integrazione della circostanza aggravante in esame non è sufficiente la titolarità della mera qualifica di pubblico ufficiale o di incaricato di pubblico servizio in capo al soggetto attivo, ma è necessario che il fatto sia commesso con abuso dei poteri o violazione dei doveri inerenti alla funzione. La qualità soggettiva quest'ultimo deve pertanto aver agevolato la realizzazione del reato[85].

In mancanza di una definizione legislativa espressa, sono sorte difficoltà in merito all'identificazione dei soggetti che ricoprono la qualità di "operatore del sistema"[86]. Escluso che possa considerarsi come tale chiunque sia venuto in contatto col sistema informatico in modo occasionale o in via continuativa[87], si ritiene che rivesta tale qualifica non solo il titolare di poteri decisori sulla gestione dei contenuti o sulla configurazione del sistema, ma anche colui che, pur se destinato a svolgere compiti meramente esecutivi, sia abilitato a operare sul sistema, modificandone i contenuti o la struttura[88].

Al n. 2, co. 2, art. 615-*ter* c.p., è punito in modo più grave il fatto commesso con violenza sulle cose, alle persone o da parte di chi è palesemente armato. Ai sensi dell'art. 392, co. 3, c.p. il concetto di violenza sulle cose, agli effetti della legge penale, comprende le ipotesi di alterazione, modificazione o cancellazione, in tutto o in parte, di un programma informatico ovvero di impedimento o turbamento del funzionamento di un sistema informatico o telematico. La circostanza aggravante in esame si applica pertanto sia nei casi di violenza fisica sull'*hardware*, sia nei casi di violenza c.d. "logica", esercitata sulla parte *software* di un sistema informatico per accedervi abusivamente[89]. Al n. 3 art. cit. è, invece, previsto un aumento di pena qualora, in conseguenza dell'accesso abusivo, derivi la distruzione, il danneggiamento o l'interruzione, in tutto o in parte, del funzionamento del sistema informatico ovvero la distruzione o il danneggiamento dei dati e dei programmi informatici in esso contenuti. Si tratta in tal caso di un reato aggravato dall'evento[90], dato che il danneggiamento non dev'essere voluto dal soggetto agente, né deve costituire il mezzo per introdursi in un sistema informatico, ma semplicemente si verifica a seguito dell'accesso

[85] Cass. pen., sez. V, sentenza 20 novembre 2020, n. 72. In tal senso v. anche SALVADORI I., *I reati contro la riservatezza informatica*, cit., p. 686.
[86] Trattasi di nozione impropria nel linguaggio informatico.
[87] PECORELLA C., *Il diritto penale dell'informatica*, cit., p. 121.
[88] Cass. pen., sez. V, sentenza 24 gennaio 2022, n. 7775.
[89] SALVADORI I., *I reati contro la riservatezza informatica*, cit., p. 687.
[90] MANTOVANI F., *Diritto penale, PS*, I, cit., p. 579.

non autorizzato[91].

Infine, il co. 3 art. cit. prevede un'ulteriore circostanza aggravante ad effetto speciale qualora il fatto riguardi sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o, comunque, di interesse pubblico.

La fattispecie di cui all'art. 615-*ter* c.p. può trovare applicazione durante l'ultima fase dei *phishing attacks*[92]. Tale disposizione non specifica la qualità, la natura o l'efficacia che deve connotare le misure di protezione del sistema, ma si limita a prevedere, quale requisito tipico del fatto di reato, la loro presenza. Non appare, dunque, esservi alcun dubbio sulla funzione protettiva delle abilitazioni necessarie per accedere a sistemi informatici (quali i nomi o i codici utente, i *pin*, le parole chiave o le *password* riservate)[93].

Si può quindi affermare l'esistenza del reato nell'ipotesi in cui l'agente, dopo aver digitato o utilizzato i privilegi o le abilitazioni collegate all'identità virtuale altrui, raggiunga un "primo livello" di contatto o connessione con il sistema, che corrisponde all'ottenimento del collegamento a seguito della verifica del profilo dell'utente utilizzato[94]. Secondo un diverso orientamento, è più corretto discutere di un accesso abusivo al sistema informatico di *home banking* del correntista (protetto da misure di sicurezza costituite dalle credenziali di accesso), così come era stato messo a disposizione dalla banca, piuttosto che di un accesso abusivo al sistema informatico di quest'ultima. Tramite le condotte di *phishing* un sistema non viene violato nella sua interezza, e neppure sarebbe "attaccato" con la semplice disponibilità delle credenziali di alcuni utenti[95].

Va, invece, esclusa l'applicabilità della norma in questione in caso di diffusione via *mail* di *virus* nel sistema informatico di tipo *spyware* o simili volti a prendere il controllo da remoto del computer della vittima. In questo caso, infatti, manca la violazione delle misure di sicurezza, in quanto è la stessa vittima che, aprendo il messaggio di posta elettronica, scarica il *virus* nel computer, per cui il reato di cui all'art. 615-*ter* c.p. non si configurerebbe[96]. Solamente se il *malware* automaticamente disabilitasse le impostazioni di sicurezza del *browser* si integrerebbe il reato in esame.

---

[91] DESTITO V., DEZZANI G., SANTORIELLO C., *Il diritto penale delle nuove tecnologie*, Padova, 2007, p. 90, che evidenziano che l'evento aggravatore in esame, proprio perché tale, non necessità copertura soggettiva dolosa.
[92] FLOR R., *Phishing e profili penali dell'attività illecita di "intermediazione" del cd. financial manager*, in *Dir. pen. proc.*, n.1, 2012, p. 55 ss., p. 60.
[93] FLOR R., *Art. 615 ter c.p*., cit., p. 107.
[94] FLOR R., *Phishing e profili penali,* cit., p. 61.
[95] CAJANI F., *Profili penali del phishing,* in *Cass. pen.*, n. 6, 2007, p. 2294 ss., p. 2297.
[96] D'ARCANGELO F., *L'accesso abusivo ad un sistema informatico*, cit., p. 1072.

3. Il reato di detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici di cui all'art. 615-*quater* c.p.

A seguito della novella legislativa del 2021, l'art. 615-*quater* c.p. punisce la detenzione e diffusione abusiva di codici di accesso informatici o telematici al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno. Al pari dell'art. 615-*ter* c.p., si tratta di un reato ostacolo, che punisce condotte prodromiche e preparatorie alla commissione di più gravi reati informatici[97]. In questo caso, però, la soglia di rilevanza penale è ulteriormente anticipata rispetto all'art. 615-*ter* c.p.

Tale fattispecie è stata novellata, sotto molteplici aspetti, dall'art. 19 l. 23 dicembre 2021, n. 238 (ovvero la c.d. legge europea 2019-2020) di attuazione della direttiva 2013/40/UE. La nuova rubrica è intitolata «*detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici*».

Tra le condotte punite vi sono la diffusione, la comunicazione o la consegna di dati elencati, ovvero condotte che si sostanziano nel mettere a disposizione i menzionati oggetti materiali[98]. Anche coloro che, una volta carpiti i dati in esame, li comunichino o, comunque, li portino a conoscenza di altri soggetti possono essere puniti. Il reato si configura come una c.d. norma a più fattispecie[99], che prevede diverse modalità alternative della condotta e un'unica ipotesi di reato, applicabile una sola volta anche in caso di realizzazione di più fattispecie. Se, pertanto, colui che ha fraudolentemente ottenuto le *password* è la stessa persona che poi le cede dietro corrispettivo, il reato sarà, comunque, unico. Tra le condotte sanzionate, infatti, vi è quella di "procurarsi" gli oggetti materiali menzionati, che consiste nell'entrare nella disponibilità con qualsiasi mezzo di un determinato oggetto[100]. La questione che si pone all'interprete è, quindi, se l'attività di "pesca" fraudolenta possa essere ricondotta sotto l'ambito applicativo della fattispecie in esame, ovvero se fra le modalità di realizzazione del fatto tipico possa essere incluso anche l'uso di un'*e-mail* che abbia un contenuto fraudolento tale da indurre il destinatario a fornire informazioni riservate[101]. A tal proposito, non sembra vi sia alcun ostacolo di sorta nel ritenere che la condotta possa consistere nell'invio di *e-mail* o nell'installazione di *malware* con lo scopo di carpire i codici

[97] SALVADORI I., *I reati contro la riservatezza informatica*, cit., p. 659.
[98] *Ibid*., p. 693.
[99] Così Cass. pen., sez. II, sentenza 20 maggio 2019, n. 21987.
[100] SALVADORI I., *I reati di possesso*, cit., p. 7 ss.
[101] FLOR R., *Phishing, identity theft,* cit., p. 909.

d'accesso[102].

Con la citata novella legislativa alle condotte precedentemente sanzionate, sono state aggiunte la detenzione (adeguando il contenuto della norma alla sua rubrica[103]), l'installazione e la messa in altro modo a disposizione di altri degli oggetti indicati dalla norma. Il richiamo alla detenzione tra le condotte tipiche è il frutto di una scelta autonoma del legislatore italiano, in quanto nella Direttiva 2013/40/UE non è espressamente prevista tra le condotte da incriminare.

Tale inserimento, tuttavia, presenta notevoli problematiche, in quanto è difficile accertare quando l'utente abbia l'effettiva disponibilità degli oggetti indicati[104]. Il problema che si pone è analogo a quello che si poneva in materia di detenzione di materiale pedopornografico, prima che il reato di cui all'art. 600-*quater* c.p. fosse modificato dall'art. 20, co. 1, lett. a), l. 23 dicembre 2021, n. 238[105], ovvero se la mera visualizzazione possa essere equiparata al possesso penalmente rilevante[106]. Se non vi è dubbio che il salvataggio dei dati della *cache* integri il fatto del possesso, anche in caso di successiva cancellazione[107], questo non è altrettanto pacifico per quei casi in cui l'utente si limita a visualizzare la pagina *Internet* e questa viene automaticamente salvata nel *browser* nei *file* temporanei. Infatti, non sempre quest'ultimo è a conoscenza del salvataggio automatico di tali dati, di cui però può comunque disporre, dato che è sufficiente accedere alla cartella dei *download* per consultare tali file.

La Cassazione in materia di detenzione di materiale pedopornografico, prima dell'intervento della citata novella legislativa, riteneva che anche il collocamento di *file* contenenti materiale pedopornografico nel "cestino" del sistema operativo del *computer*

---

[102] *Ibid*.

[103] Prima di tale modifica era dibattuto in dottrina se la mera detenzione di codici di accesso fosse sanzionata o meno dalla norma. In senso favorevole v. MANTOVANI F., *Dir. pen, P.S.*, I, p. 580; CANNATA S., COSTALUNGHI D., *Detenzione e diffusione di codici d'accesso a sistemi informatici o telematici (art. 615-quater)*, in *Trattato di diritto penale- parte speciale*, vol. IX - *I delitti contro la libertà sessuale, la libertà morale, l'inviolabilità del domicilio e l'inviolabilità dei segreti*, a cura di A. Cadoppi, S. Canestrari, A. Manna e M. papa, Torino, 2011, p. 553 ss., p. 555. In senso contrario v. SALVADORI I., *I reati contro la riservatezza informatica*, cit., p. 694 s. e PARODI C., *I reati patrimoniali*, p. 147.

[104] SALVADORI I., *I reati di possesso*, cit., p. 85.

[105] L'art. 20 cit., infatti, ha inserito un nuovo co. 3 nell'art. 600-*quater* c.p., il quale recita «*Fuori dei casi di cui al primo comma, chiunque, mediante l'utilizzo della rete internet o di altre reti o mezzi di comunicazione, accede intenzionalmente e senza giustificato motivo a materiale pornografico realizzato utilizzando minori degli anni diciotto è punito con la reclusione fino a due anni e con la multa non inferiore a euro 1.000*». A seguito della novella legislativa in questione è pertanto pacifico che anche la mera visualizzazione di file contenenti materiale pedopornografico sia penalmente rilevante.

[106] *Ibidem*, p. 86 ss.

[107] Cass. pen., sez. III, sentenza 29 novembre 2021, n. 43615; Cass. pen., sez. III, sentenza 19 marzo 2021, n. 10759; Cass. pen., sez. III, sentenza 14 gennaio 2019, n. 1509; Cass. pen., sez. III, sentenza 8 marzo 2017, n. 11044.

integrasse la condotta di detenzione, perché questi restano comunque disponibili mediante la semplice riattivazione dell'accesso al *file*[108]. Pertanto, poiché anche quando il *file* si è automaticamente scaricato nel computer questo è comunque a disposizione dell'utente, che lo può in qualsiasi momento trovare nell'apposita cartella e aprire, si può ritenere che in quest'ipotesi si configuri il possesso penalmente rilevante, anche ai sensi dell'art. 615-*quater* c.p.

Tuttavia, va evidenziato che, a seguito della citata novella legislativa di cui all'art. 20 l. 238/2021, il legislatore ha aggiunto la condotta di accesso a quelle sanzionate dall'art. 600-*quater* c.p., condotta che, dunque, viene ad affiancarsi a quella di detenzione, già punita. La mancata menzione di tale condotta nell'art. 615-*quater* c.p. rende quindi evidente che la mera visualizzazione di *password* idonee all'accesso al computer altrui senza essere scaricate non configuri possesso penalmente rilevante.

In caso di mancata conoscenza dell'avvenuto trasferimento va comunque tenuto presente che la norma richiede il dolo specifico del «*fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno*», per cui in questo caso difetterebbe comunque l'elemento soggettivo e non si configurerebbe comunque il possesso penalmente rilevante[109]. Per quanto riguarda l'elemento soggettivo, va specificato che il profitto non dev'essere necessariamente di natura patrimoniale. Invece, il fine di arrecare un danno esso non è riferito alla volontà di rendere danneggiare, alterare o rendere inservibili i dati o i programmi in esso contenuti (finalità tipica del diverso reato di cui all'art. 615-*quinquies* c.p.), ma si riferisce alla volontà di ottenere indebitamente informazioni da utilizzare per ledere il titolare delle stesse[110].

Con l'aggiunta della detenzione alle condotte sanzionate, il legislatore ha scelto di punire anche coloro che, senza essersi procurati o senza farne uso, si limitano a disporre dei dispositivi ivi elencati idonei all'accesso al sistema informatico. Tale estensione dell'ambito applicativo della norma presenta difficoltà anche sotto il profilo del rispetto dei principi di offensività e di proporzione[111].

È evidente che lo scopo politico-criminale di questa incriminazione sia quello di

---

[108] Cass. pen., sez. III, sentenza 29 novembre 2021, n. 43615, cit.; Cass. pen., sez. III, sentenza 21 aprile 2015, n. 24345; Cass. pen., sez. III, 6 ottobre 2010, n. 639.

[109] In tal senso anche SALVADORI I., *I reati di possesso*, cit., p. 87 s.

[110] SALVADORI I., *I reati contro la riservatezza informatica*, cit., p. 698.

[111] V. PECORELLA C., *Diritto penale dell'informatica*, II ed., Padova, 2006, p. 359 ss., che già nella sua vecchia formulazione riteneva l'art. 615-*quater* c.p. «*difficilmente conciliabile col principio di proporzione*» in ragione dell'eccessiva anticipazione della tutela penale. Negli stessi termini anche FUMO M., *La condotta nei reati informatici*, cit., p. 782.

impedire l'utilizzo dei menzionati oggetti detenuti per commettere un più grave reato, ovvero l'accesso abusivo al sistema informatico-telematico, il quale a sua volta può preludere alla commissione di ulteriori illeciti. Tuttavia, la detenzione è di per sé una condotta c.d. neutra, che non presenta disvalore sociale[112]. Dunque, qui è la previsione del fine criminoso che assolve ad una funzione selettiva dei comportamenti penalmente illeciti rispetto a quelli leciti, la condotta oggettiva rappresenta un "mezzo" strumentale al perseguimento di un fine soggettivamente tipizzato[113]. Pertanto, il rischio è che l'elemento soggettivo finisca inammissibilmente per essere presunto sulla base della mera presenza di tali dati all'interno del sistema informatico.

Va però evidenziato che già nella sua precedente formulazione l'art. 615-*quater* conteneva la clausola d'illiceità speciale dell'abusività delle condotte, abusività che dev'essere intesa come contrarietà alle norme extra penali che disciplinano l'attività dei soggetti che operano nel settore informatico[114]. Il carattere abusivo conferisce alla detenzione una speciale connotazione negativa, arricchendo il fatto tipico qualificandolo in termini sia oggettivi che soggettivi. Pertanto, rispetto a tale ipotesi criminosa, oltre al dolo specifico richiesto dalla norma, che però non riesce a delimitare adeguatamente l'ambito del penalmente rilevante[115], è necessaria anche la consapevolezza del carattere penalmente illecito della detenzione di un determinato oggetto tra quelli indicati dall'art. 615-*quater* c.p. e del suo disvalore per un interesse giuridico, che presuppone la conoscenza attuale della normativa extra penale di riferimento. Tale elemento essenziale, che concorre a descrivere il fatto di reato, deve rientrare nell'oggetto del dolo, impedendo così inammissibili presunzioni di colpevolezza. Peraltro, va aggiunto che tale inserimento nulla apporta sul piano della criminalizzazione delle diverse fasi degli attacchi informatici. Infatti, trattandosi, come evidenziato, di una norma a più fattispecie, essa è applicabile una sola volta anche in caso di realizzazione di più fattispecie. Se, pertanto, colui che ha fraudolentemente ottenuto le *password* è la stessa persona che poi le cede dietro corrispettivo, come peraltro è la prassi, poiché appare piuttosto arduo ipotizzare che un soggetto si limiti a possedere tali dati senza esserseli procurati, il reato sarà comunque unico.

È invece apprezzabile l'aggiunta dell'installazione alle condotte sanzionate, data

[112] SALVADORI I., *I reati di possesso,* cit., p. 101.
[113] PICOTTI L., *Il dolo specifico,* cit., p. 501.
[114] PICOTTI L., *Internet e diritto penale: il quadro attuale alla luce dell'armonizzazione internazionale*, in *Dir. dell'Internet*, 2005, n. 2, p. 189 ss., p. 197; SALVADORI I., *I reati contro la riservatezza informatica*, cit., p. 696.
[115] SALVADORI I., *I reati contro la riservatezza informatica,* cit., p. 696.

l'ampia diffusione delle *App* di autenticazione per l'accesso a determinati servizi *online*, così come della clausola di chiusura «*mette in altro modo a disposizione di altri*», che permette di ricondurre nell'ambito applicativo della fattispecie i comportamenti che consistono nel mettere a disposizione con qualsiasi modalità qualsiasi mezzo idoneo all'accesso al sistema informatico o telematico.

Oggetto materiale del reato in questione sono i codici, le parole chiave o gli altri mezzi, le indicazioni o le informazioni idonei all'accesso ad un sistema informatico o telematico protetto da misure di sicurezza e, a seguito della novella legislativa, anche «*apparati, strumenti, parti di apparati o strumenti*». A ben guardare, però, anche tali oggetti già potevano rientrare nella clausola di chiusura estremamente elastica già presente nella norma. Anzi, questa modifica paradossalmente complica il lavoro degli interpreti, perché la direttiva fa riferimento alle diverse nozioni di "sistema di informazione" e "dati informatici"[116]. La giurisprudenza già in passato ha evidenziato la loro natura di categorie aperte e dinamiche, suscettibili di essere implementate per effetto delle innovazioni tecnologiche[117]. Si ritiene, dunque, che gli apparati altro non siano che apparecchiature per accedere al sistema informatico, mentre gli strumenti siano i programmi per computer[118]. Il concetto di "parola chiave" in questo caso va inteso come *password* o codice d'accesso, ovvero mezzo che permette di collegarsi al sistema[119].

Tra gli «*altri mezzi idonei all'accesso*» si può includere anche l'indirizzo *e-mail* o il numero di carta di credito, ove svolgano le funzioni tipiche di identificazione dell'utente per abilitarlo all'accesso ai servizi *online*, normalmente abbinati ad una *password* o parole chiave. Secondo la Cassazione anche i numeri telefonici ed i numeri seriali dei cellulari costituiscono codici di accesso a un sistema informatico o telematico ai sensi della norma in esame, in quanto permettono di individuare l'utenza e l'apparato cui è abbinata e, per il loro tramite, laddove abusivamente replicati su un altro apparecchio tramite clonazione, è possibile realizzare una illecita connessione alla rete di telefonia mobile, che costituisce un sistema telematico protetto[120]. Ciò significa che questa fattispecie è idonea a sanzionare anche la clonazione dei *token* virtuali installati sullo *smartphone*.

La Cassazione, inoltre, ritiene che nell'ambito applicativo del reato in questione

---

[116] Così FUMO M., *La condotta nei reati informatici*, cit., p. 775 ss., che critica l'utilizzo da parte del legislatore in quest'ambito di termini "vaghi e indeterminati", spesso erroneamente tradotti dalla lingua inglese.
[117] Cass. pen., sez. V, sentenza 5 aprile 2019, n. 15071.
[118] V. la *Relazione dell'Ufficio del Massimario presso la Corte di cassazione* n. 20 del 2022, p. 6.
[119] FLOR R., Sub. *Art. 615-quater c.p.*, in *Commentario breve al codice penale*, a cura di G. Forti, S. Seminara e G Zuccalà, VI ed., Padova, 2017, p. 2133 ss., p. 2134.
[120] Cass. pen., sez. II, sentenza 17 dicembre 2004, n. 5688.

rientri anche l'illecita apprensione di codici o di altri dati relativi a carte di credito o di debito utilizzate da utilizzare per prelevare il danaro contante attraverso il sistema bancomat, ritenuto anch'esso sistema informatico o telematico[121]. Quest'interpretazione, tuttavia, come si esaminerà nel prosieguo, crea difficoltà di coordinamento con le fattispecie poste a tutela specifica delle carte di credito.

Per quanto riguarda le pene previste, l'art. 19 cit. ha poi aumentato la pena detentiva per il reato base, che ora è punito con la reclusione sino a due anni.

Le modifiche hanno poi riguardato anche le circostanze aggravanti: il precedente richiamo di cui al co. 2 dell'art. 615-*quater* c.p. alle ipotesi aggravate di cui all'art. 617-*quater* c.p. è stato ampliato sino a ricomprendere l'ipotesi del fatto commesso da chi esercita abusivamente la professione di investigatore privato. Dunque, le circostanze aggravanti ad effetto speciale non sono più unicamente relative ai dati idonei a consentire l'accesso ad un sistema informatico utilizzato dallo Stato o da una impresa esercente un servizio pubblico o di pubblica utilità e al fatto posto in essere da un agente pubblico con abuso dei suoi poteri o con violazione dei suoi doveri ovvero con abuso della qualità di operatore del sistema. Inoltre, il massimo edittale delle ipotesi aggravate è stato elevato a tre anni di reclusione.

Si può dunque ritenere che questa fattispecie sia applicabile alla prima fase dei *phishing attacks* (v. *supra* cap. I, par. 6): proprio perché trattasi di reato a dolo specifico, per la consumazione del reato non è necessaria la realizzazione oggettiva del fine, essendo sufficiente la sola volontà di agire per il perseguimento di quel profitto o per arrecare un danno. È possibile quindi affermare la sussistenza dell'illecito penale già nel caso in cui il reo si procuri, riproduca, diffonda questi codici, anche se successivamente non ne tragga profitto, per sé o altri, o non ne faccia un uso indebito o non effettui un accesso senza autorizzazione ai servizi finanziari o bancari *online*[122].

La fattispecie in esame trova applicazione anche durante la seconda fase dei *phishing attacks*. Infatti, come evidenziato, tra le condotte punite vi sono la diffusione, comunicazione o consegna dei dati elencati, ovvero condotte che si sostanziano nel mettere a disposizione i menzionati oggetti materiali. Dunque, la vendita delle credenziali altrui nel *dark web* rientra nell'ambito applicativo della norma in questione. Si deve però tener presente che il reato in questione è una c.d. norma a più fattispecie, per cui se colui che ha fraudolentemente ottenuto le password è la stessa persona che poi le cede dietro corrispettivo, il reato sarà comunque

[121] Cass. pen., sez. II, sentenza 3 ottobre 2013, n. 47021.
[122] FLOR R., *Phishing, identity theft,* cit., p. 909. Più recente v. anche SALVADORI I., *Il diritto penale dei software "a duplice uso"*, cit., p.396 ss.

unico. Per questo motivo, non si può ritenere che la norma in questione sia idonea a sanzionare la seconda fase dei *phishing attacks*, anche in ragione del blando trattamento sanzionatorio.

4. I rapporti concorsuali

La scelta del legislatore di non inserire alcuna clausola di sussidiarietà all'interno dell'art. 615-*quater* c.p. rende assai problematici i rapporti tra quest'ultima fattispecie e l'art. 615-*ter* c.p.

Poiché, come si è sopra esaminato, quest'ultimo reato consiste nell'introduzione abusiva in un sistema informatico o telematico protetto da misure di sicurezza, è evidente che l'autore, salvo non li possegga già per altri motivi, debba necessariamente di procurarsi i codici d'accesso al sistema informatico o telematico altrui. Tale ultima condotta, tuttavia, è già sanzionata dal diverso reato di cui all'art. 615-*quater* c.p. Dunque, la condotta di colui che, dopo essersi procurato illecitamente le credenziali altrui, accede abusivamente ad un sistema informatico o telematico, è astrattamente riconducibile sia alla fattispecie di cui all'art. 615-*ter* c.p., sia a quella di cui all'art. 615-*quater* c.p. Si deve, pertanto, verificare quale sia il rapporto tra le due fattispecie descritte e se le stesse concorrano o meno tra loro.

Per prima cosa si deve rilevare che i due reati si consumano in momenti fisiologicamente diversi, perché l'accesso abusivo si consuma con l'effettivo accesso non autorizzato al sistema, mentre il reato di cui all'art. 615-*quater* c.p. si realizza nel momento in cui il soggetto carpisce i codici d'accesso. Secondo il criterio della specialità, questo è sicuro indice dell'autonomia delle due fattispecie, il che preclude la possibilità di configurare il concorso apparente di norme[123]. Inoltre, è evidente che il procurarsi i codici d'accesso non è elemento costitutivo del reato di accesso abusivo. Per tale motivo, in assenza di clausola di riserva, se si aderisce alla tesi monista per la quale l'unico criterio utilizzabile ai fini dell'identificazione del concorso apparente di norme è quello della specialità, si deve necessariamente concludere per il concorso tra le due fattispecie, come ritiene una parte della giurisprudenza[124]. In tale contesto, dunque, l'autore di un accesso abusivo dovrà sempre

[123] Cass. pen., sez. un., sentenza 7 giugno 2001, n. 23427: il fatto che i reati si consumino fisiologicamente in tempi diversi è un rilevante indicatore dell'autonomia delle fattispecie, preclusivo di un rapporto di identità tra norme suscettibile di qualificare un concorso apparente. In dottrina v. DE FRANCESCO G., *Lex specialis. Specialità ed interferenza nel concorso di norme penali*, Milano, 1980, p. 68, che evidenzia che nelle ipotesi in cui la diversità concerne l'elemento della condotta, le condotte sono attuate l'una successivamente all'altra, dando vita ad una pluralità di azioni. Pertanto, in assenza di unità di azione, non si può che configurare un concorso materiale di reati.

[124] Cass. pen., sez. II, sentenza 25 settembre 2008, n. 36721.

rispondere anche del reato di cui all'art. 615-*quater* c.p., con la sola esclusione del caso in cui l'autore sia un *intraneus* che possegga le credenziali per essergli state fornite dallo stesso titolare e ne faccia quindi indebito uso.

Tale soluzione non appare però soddisfacente in quanto l'art. 615-*quater* c.p. è reato di pericolo indiretto con funzione di tutela anticipata, che reprime, indipendentemente dal verificarsi dell'evento, condotte prodromiche della realizzazione del delitto di accesso abusivo in un sistema informatico o telematico protetto da misure di sicurezza. Inoltre, il bene giuridico protetto da entrambe le norme è il medesimo, ovvero la riservatezza informatica. Sostanzialmente, quindi, gli artt. 615-*ter* e 615-*quater* c.p. sono due norme volte a sanzionare le diverse fasi dello stesso fenomeno criminoso, ovverosia il *phishing* nelle sue molteplici varianti, nel quale i criminali dapprima creano *e-mail* o siti abilmente contraffatti per carpire le *password* altrui e dopo, una volta ottenute, le utilizzano per entrare nel sistema di *home banking* sostituendosi all'ignaro correntista. Si deve quindi rilevare che le due fattispecie sono tra loro in rapporto di stretta connessione: infatti, il "procurarsi" i codici d'accesso costituisce necessario antefatto dell'accesso abusivo, ad eccezione, come detto, dei soli casi in cui il reo sia già lecitamente in possesso delle credenziali. In tale contesto, ove il disvalore penale è sostanzialmente omogeneo, l'applicazione del solo principio di specialità non solo non è risolutiva, ma finisce per dar vita ad una moltiplicazione di sanzioni che è difficilmente giustificabile. Non mancano, dunque, le opinioni dottrinali sensibili alle esigenze di giustizia sostanziale e favorevoli all'assorbimento tra i due reati[125]. A tale ultimo orientamento ha aderito anche la giurisprudenza più recente, che ha ritenuto che i due reati non possano concorrere, in quanto «*il reato di cui all'art. 615 quater costituisce necessario antefatto del reato di cui all'art. 615 ter, poiché le due fattispecie criminose si pongono in stretta connessione, tutelando entrambe il medesimo bene giuridico, ovvero il domicilio informatico, passando da condotte meno invasive a condotte più invasive, poiché indiscriminate, che, sotto un profilo naturalistico, necessariamente presuppongono le prime*»[126]. Per la Suprema Corte, dunque, tra i due reati vi sarebbe progressione criminosa in senso stretto, che sussiste quando, ferma l'unità di contesto e l'identità del soggetto passivo, la progressione avviene per effetto di risoluzioni criminose successive. Pertanto, è stato ritenuto applicabile il criterio dell'assorbimento, evidenziando che nell'ambito del

[125] FLOR R., *phishing, identity theft e identity abuse. Le prospettive applicative del diritto penale vigente*, in *Riv. it. dir. proc. pen.*, 2007, n. 2-3, p. 899 ss., 911; PECORELLA C., Il diritto, p. 374.; CAJANI F., *Profili penali del phishing, in Cass. pen.*, 2007, n. 6, p. 2294 ss., p. 2297. DOLCINI E., GATTA G.L., *Commentario al codice penale*, p. 610.
[126] Cass. pen., sez. II, sentenza 20 maggio 2019, n. 21987.

fenomeno criminoso del *phishing* la commissione dell'accesso abusivo implica necessariamente il passaggio attraverso un'altra ipotesi delittuosa, ovvero l'art. 615-*quater* c.p. Secondo tale prospettiva, quindi, risponderebbero del reato di detenzione e diffusione abusiva di codici d'accesso ex art. 615-*quater* c.p. unicamente coloro che si limitano a procurarsi, riprodurre, diffondere, ecc. codici d'acceso e *password*, fenomeno autonomo che, peraltro, oggi è assai rilevante, dato che vi sono vere e proprie associazioni a delinquere dedite alla vendita nel *deep web* di dati altrui illecitamente carpiti con attività di *hacking* e *phishing*.

La configurabilità dell'assorbimento sembra trovare conferma anche in quelli che sono i limiti edittali previsti da entrambe le fattispecie, nonostante il recente innalzamento della pena per il reato di cui all'art. 615-quater da parte della l. 238/2021: infatti, l'art. 615-*quater* c.p. nella sua ipotesi base è punito con la reclusione sino ad due anni e con la multa sino ad euro 5.164,00, mentre l'art. 615-*ter* c.p., sempre nell'ipotesi base, prevede la reclusione fino a tre anni, per cui, da tale punto di vista, non vi sono ostacoli nel ritenere che il reato meno grave di cui all'art. 615-*quater* c.p. sia assorbito nel diverso reato di accesso abusivo a sistema informatico o telematico. Peraltro, va evidenziato che in passato una parte della giurisprudenza ha fatto uso del principio dell'assorbimento proprio con riferimento a diverse ipotesi criminose simili a quelle in esame, tra cui il possesso ingiustificato di arnesi atti allo scasso nel delitto di furto aggravato dalla violenza sulle cose, per contenere gli effetti del concorso di reati[127].

Nonostante tale ultimo orientamento sia assolutamente condivisibile, si deve però rilevare che quest'ultima interpretazione della Cassazione, malgrado la volontà contraria degli estensori[128], si pone in oggettivo contrasto con l'interpretazione monista, prevalente e da ultimo ribadita dalle recenti pronunce delle Sezioni Unite[129], poiché applica un criterio diverso rispetto a quello della specialità, ovvero quello di consunzione-assorbimento.

In ogni caso resta poi irrisolto il problema della diversa procedibilità tra i due reati: la stessa giurisprudenza che ha ammesso la configurabilità dell'assorbimento del reato di cui all'art. 615-*quater* c.p. nell'art. 615-*ter* c.p., ha evidenziato che qualora il reato più grave

[127] Cass. pen., sez. II, sentenza 15 aprile 1998, n. 6955; Cass. pen., sez. V, sentenza 30 giugno 2015, n. 431; Cass. pen., sez. V, sentenza 19 febbraio 2010, n. 19047.
[128] In verità, per cercare di evitare l'aperto conflitto, la seconda sezione sostiene che il criterio dell'antefatto non punibile sia riconducibile al criterio della specialità ai sensi dell'art. 15 c.p., ma il risultato è comunque quello di intendere il concetto di "stessa materia" in modo differente rispetto al dettato delle Sezioni Unite, le quali adottano un'interpretazione restrittiva.
[129] V. Cass. pen., sez. un., 23 febbraio 2017, n. 20664, cit. e Cass. pen., sez. un., 12 settembre 2017, n. 41588, cit.

non sia punibile, il reo dovrebbe comunque per rispondere del reato meno grave, dato che l'assorbimento attiene unicamente al fatto concreto. A tal proposito, la procedibilità d'ufficio dell'art. 615-*quater* c.p. può trovare giustificazione nella difficoltà per tutti gli ignari utenti di venire a sapere che le loro credenziali di accesso sono state illecitamente carpite e quindi sporgere querela. È però evidente che, in caso di rimessione di querela, possibile per il solo reato di cui all'art. 615-*ter* c.p., l'autore del fatto dovrebbe comunque rispondere del reato di detenzione e diffusione abusiva di codici d'accesso, nonostante la volontà contraria della persona offesa ai danni della quale è avvenuto l'accesso abusivo, conseguenza assolutamente iniqua.

5. Il nuovo reato di detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti di cui all'art. 493-quater c.p.

Il menzionato d.lgs. 8 novembre 2021 n. 184, di attuazione della direttiva 2019/713/UE dedicata alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti, ha introdotto all'art. 493-*quater* c.p. il nuovo delitto di «*detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti*».

La fattispecie in esame, a differenza delle altre sopra menzionate, è collocata tra i delitti contro la fede pubblica, in particolare nel capo III dedicato alla falsità in atti, per cui beni giuridici tutelati dalle norme sono sia la fede pubblica, sia la sicurezza delle transazioni commerciali elettroniche, interesse collettivo indisponibile dal privato[130]. Per questo motivo, dunque, non opera la scriminante del consenso dell'avente diritto.

Tale norma sanziona chiunque, al fine di farne uso o di consentirne ad altri l'uso nella commissione di reati riguardanti strumenti di pagamento diversi dai contanti, produce, importa, esporta, vende, trasporta, distribuisce, mette a disposizione o in qualsiasi modo procura a sé o ad altri apparecchiature, dispositivi o programmi informatici che, per caratteristiche tecnico-costruttive o di progettazione, sono costruiti principalmente per commettere tali reati, o sono specificamente adattati al medesimo scopo. Il legislatore non ha individuato le specifiche fattispecie per quali strumenti in questione debbano essere

[130] NATALINI A., *Va in soffitta il riferimento alle carte e si fa largo la dematerializzazione. Profili sanzionatori*, in *Guida dir*., 2021, n. 49-50, p. 38 ss., p. 40.

specificamente progettati o adattati; pertanto, si ritiene possano essere reati contro la fede pubblica, contro il patrimonio o che comunque offendono il patrimonio[131].

Vi è poi una discrasia tra la rubrica della norma e le condotte sanzionate. Infatti, la mera detenzione di apparecchiature, dispositivi e programmi non è indicata nel testo tra le condotte punite, ma lo è solo la produzione, alla quale non può essere assimilato il mero possesso[132]. Anche tale reato costituisce una c.d. norma a più fattispecie, per cui le condotte ivi elencate sono sanzionate tra loro in via alternativa[133].

Trattasi, dunque, sulla falsariga dell'art. 615-*quater* c.p., di reato di pericolo che sanziona condotte prodromiche alla commissione di ulteriori illeciti relativi agli strumenti di pagamento diversi dai contanti. Il parallelismo con quest'ultima fattispecie è evidente: anche in questo caso la tutela penale viene anticipata e l'elemento soggettivo previsto è il dolo specifico, al fine di delimitare l'ambito del penalmente rilevante[134]. In questo caso, però, il reo deve agire «*al fine di farne uso o di consentirne ad altri l'uso nella commissione di reati riguardanti strumenti di pagamento diversi dai contanti*». Una differenza significativa risiede nel fatto che, a differenza dell'art. 615-*quater* c.p.[135], nel nuovo art. 493-*quater* c.p. è stata espressamente inserita la clausola di sussidiarietà «*salvo che il fatto costituisca più grave reato*», rendendo così esplicito il rapporto di sussidiarietà tra tale fattispecie e il più grave reato di indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti. Inoltre, il legislatore italiano ha specificato che gli oggetti del reato debbono essere «*costruiti principalmente per commettere tali reati, o […] specificamente adattati al medesimo scopo*». In tal modo, ha preso atto del fatto che molti dei programmi utilizzati per commettere reati possono avere finalità del tutto lecite e ha voluto selezionare i *software* oggettivamente configurati per commettere attività illecite, delimitando così l'ambito del penalmente rilevante. Peraltro, la stessa direttiva 713/2019/UE evidenziava la necessità di evitare una criminalizzazione di tali strumenti ove prodotti e posti in commercio per fini

[131] BERNARDONI P., *Attuazione degli obblighi europei in materia di lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti: prima lettura del d.lgs. n. 184 del 2021*, in *Sist. pen*., 3 febbraio 2021.
[132] Cft. SALVADORI I., *I reati contro la riservatezza informatica*, cit., p. 694, che evidenzia come il "procurarsi" concerna attività che precedono logicamente la detenzione.
[133] NATALINI A., *Va in soffitta il riferimento alle carte*, cit., p. 40.
[134] Sulla struttura e sul ruolo del dolo specifico v. PICOTTI L., *Il dolo specifico. Un'indagine sugli "elementi finalistici" delle fattispecie penali*, Milano, 1993, p. 471 ss.
[135] In mancanza di clausola di sussidiarietà espressa, i rapporti tra gli artt. 615-*ter* e 615-*quater* c.p. sono tuttora controversi. Per Cass. pen., sez. II, sentenza 20 maggio 2019, n. 21987 i due reati non possono concorrere in quanto il reato di cui all'art. 615- *quater* costituirebbe necessario antefatto del reato di cui all'art. 615-*ter*. Al contrario per Cass. pen., sez. II, sentenza 25 settembre 2008, n. 36721 possono concorrere in quanto non sono tra loro in rapporto di specialità.

legittimi, sostenendo pertanto che la criminalizzazione dovrebbe essere limitata agli strumenti principalmente concepiti o specificamente adattati al fine di commettere i reati di cui alla presente direttiva[136]. Se da un lato tale tentativo è apprezzabile, dall'altro va però segnalato che, come sopra evidenziato (v. *supra* par. 1), non è affatto agevole individuare quando un programma informatico sia stato concepito o adattato principalmente per commettere un reato.

L'introduzione di questa nuova fattispecie crea difficoltà applicative con riferimento ai rapporti col reato di cui all'art. 615-*quater* c.p.[137] Quest'ultimo reato, infatti, in giurisprudenza veniva ritenuto pacificamente applicabile all'illecita acquisizione di codici di carte di credito e bancomat[138]. Questo perché il concetto di "parola chiave" viene da sempre inteso come *password* o codice d'accesso, ovvero mezzo che permette di collegarsi al sistema[139]. Per cui tra gli «*altri mezzi idonei all'accesso*» si può includere anche l'indirizzo *e-mail* o il numero di carta di credito, che svolgono le funzioni tipiche di identificazione dell'utente per abilitarlo all'accesso ai servizi *online*, normalmente abbinati con *password* o parole chiave.

Dunque, la fattispecie di nuova introduzione, che si limita a far riferimento all' "uso nella commissione di reati" senza però specificare quali, si pone in rapporto d'interferenza con l'art. 615-*quater* c.p. Poiché i due reati hanno pena identica, la clausola di sussidiarietà di cui all'art. 493-*quater* c.p. non può trovare applicazione. Inoltre, da quando la l. 23 dicembre 2021, n. 238 ha ampliato l'oggetto del reato di cui all'art. 615-*quater* c.p., aggiungendovi proprio le "apparecchiature" e gli "strumenti" (nei quali possono dunque essere ricompresi i dispositivi o programmi informatici), esso viene a coincidere con quello di cui all'art. 493-*quater* c.p. È difficile individuare un rapporto di specialità tra le due le fattispecie, perché appaiono strutturalmente molto differenti, anche se l'oggetto del reato di cui all'art. 615-*quater* c.p. è più ampio perché ricomprende anche l'acquisizione delle mere *password* e dei codici d'accesso. Inoltre, tali oggetti debbono essere specificamente idonei a consentire l'accesso ad un sistema informatico o telematico, non semplicemente a commettere reati come quelli di cui all'art. 493-*quater* c.p.

---

[136] V. considerando n. 10 e 17 della direttiva.

[137] Tali possibili frizioni erano già state segnalate da VADALÀ R.M., *La tutela penale della sicurezza degli scambi economici digitali*, Università degli Studi di Verona, Dipartimento di Scienze Giuridiche, formato ebook-cod. ISBN 9788899957025, ottobre 2021, p. 58 ss. con riferimento allo schema di attuazione del decreto legislativo.

[138] Cft. Cass. pen., sez. II, sentenza 3 ottobre 2013, 47021.

[139] FLOR R., *Sub Art. 615-quater c.p.*, in *Commentario breve al codice penale*, a cura di G. Forti, S. Seminara e G Zuccalà, VI ed., Padova, 2017, p. 2133 ss., p. 2134.

Tuttavia, appare arduo tracciare il *discrimen* tra i due reati sulla base dell'idoneità o meno dell'apparecchio o programma informatico a consentire l'accesso abusivo, perché si tratta di una differenza assai labile. Infatti, nella maggior parte dei casi, per realizzare una frode informatica o comunque avente ad oggetto mezzi di pagamento diversi dai contanti, è comunque necessario realizzare un accesso abusivo al sistema informatico o telematico, basti pensare al classico *hacker* che costruisce un programma di tipo *spyware*, che poi invia alle sue vittime invitandole a cliccare su un *link* fasullo ed installa così il *virus* che intercetta le loro credenziali e gli consente di avere l'accesso al loro sistema di *home banking*. Tale condotta, infatti, può astrattamente essere riconducibile ad entrambe le fattispecie.

Va però evidenziato che l'elemento soggettivo dei due reati è diverso: infatti, nel caso dell'art. 615-*quater* c.p. è necessario che il fine criminoso sia quello di procurare a sé o ad altri un ingiusto profitto, mentre quello di cui all'art. 493-*quater* c.p. è semplicemente quello di fare uso di tali strumenti nella commissione di reati. Dunque, il *discrimen* tra le due fattispecie potrebbe essere individuato proprio nel fine perseguito dall'agente, anche se, all'atto pratico, appare difficile distinguere i casi in cui il reo si procura un dispositivo atto ad intercettare le credenziali altrui per trarne profitto, magari per vendere le credenziali altrui nel *darkweb*, oppure per utilizzarlo per commettere ulteriori reati.

D'altra parte, anche se non si può ritenere che tra le due fattispecie vi sia un rapporto di sussidiarietà, non sembra comunque ragionevole ritenere che i due reati debbano necessariamente concorrere, pena una irragionevole ed ingiustificata duplicazione sanzionatoria. Infatti, l'oggetto dell'art. 615-*quater* c.p. è più ampio, perché contempla anche le sole *password* e i codici d'accesso, per cui nel caso in cui il reo si limiti a disporre di codici e *password* si configurerebbe solo quest'ultima fattispecie. Dunque, non appare giustificato che, invece, nel caso in cui il reo disponga di un programma di tipo *spyware* o di uno *skimmer,* al posto che del singolo codice d'accesso, debba rispondere di entrambi i reati.

6. La diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico di cui all'art. 615-*quinquies* c.p.

Altro reato introdotto dalla l. 23 dicembre 1993 n. 547 è il reato di cui all'art. 615-*quinquies* c.p. La fattispecie in questione è stata oggetto di modifiche sia da parte della l. 18 marzo 2008 n. 48 di attuazione della Convenzione *cybercrime*, sia da parte dell'art. della l. 23 dicembre 2021, n. 238 di attuazione della direttiva 2013/40/UE. Tale norma, considerata

una delle più innovative fattispecie inserite dal legislatore del 1993[140], fu inserita nel codice allo scopo di anticipare la soglia di punibilità rispetto all'effettivo "danneggiamento" di dati o di sistemi[141].

A differenza di quanto sopra evidenziato per i reati di cui agli artt. 615-*ter* e *quater* c.p., questo è un reato necessariamente prodromico alla commissione di un danneggiamento informatico, ove il bene giuridico tutelato è l'integrità di dati e sistemi informatici[142]. Dunque, la sua collocazione è stata criticata in dottrina perché non coerente con la *ratio* della norma[143].

Trattasi di reato di pericolo eventualmente indiretto, dato che la diffusione di un virus può avere sia un effetto immediato sul sistema o sul funzionamento del sistema informatico, sia essere oggetto di ulteriore diffusione, con conseguente pericolo per un numero indefinito di sistemi informatici[144]. Data l'elevata importanza della tutela dell'integrità e del buon funzionamento dei sistemi informatici nella società odierna, si concorda con coloro che ritengono che l'anticipazione della tutela non contrasti col principio di proporzione[145].

Come accennato, l'art. 615-*quinquies* c.p. è stato modificato in modo significativo dall'art. 19 l. 238/2021 cit., a partire dalla sua rubrica, che è ora intitolata «*detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico*». Alle condotte previamente sanzionate dalla norma a seguito della novella di cui alla l. 48/2008 cit.[146], ovvero il procurarsi, la produzione, la riproduzione, l'importazione, la diffusione, la comunicazione e la consegna, sono state aggiunte la detenzione e l'installazione degli oggetti ivi indicati, mentre "la messa a disposizione di altri" è stata ampliata tramite l'aggiunta della

---

[140] PICOTTI L., *La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale*, in *Dir. pen. proc*., 2008, n. 6, p. 700 ss., p. 708.
[141] PECORELLA C., *Diritto penale,* cit., p. 236.
[142] Così PICOTTI L., *Sistematica dei reati informatici*, cit., p. 70; SALVADORI I., *Il "microsistema" normativo concernente i danneggiamenti informatici. Un bilancio molto poco esaltante*, in *Riv. it. dir. e proc. pen*., 2012, n. 1, p. 204 ss., p. 238; CAPPELLINI A., *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici*, in *Cybercrime*, cit., p. 761 ss., p. 777; PICA G., *Diritto penale delle tecnologie informatiche*, cit., p. 109.
[143] In tal senso PICA G., *Diritto penale delle tecnologie informatiche*, cit., p. 109; SALVADORI I., *I reati contro la riservatezza informatica*, cit., p. 701; PICOTTI L., *La ratifica della Convenzione Cybercrime*, cit., p. 708. Unico autore dissenziente è GALDIERI P., *Teoria e pratica nell'interpretazione del reato informatico*, cit., p. 160, secondo cui l'articolo in esame rafforzerebbe la tutela del c.d. "domicilio informatico".
[144] PECORELLA C., *Diritto penale,* cit., p. 236 s.; PERRI P., *Sub art. 615-quinquies c.p.*, in *Commentario breve al codice penale*, cit., p. 2135 ss., p. 2136.
[145] PECORELLA C., *Diritto penale,* cit., p. 236 s.
[146] Prima di tale novella la norma in questione sanzionava unicamente i comportamenti finalizzati a "ottenere la disponibilità" di tali programmi, ovvero la diffusione, la comunicazione e la consegna, in palese contraddizione con la volontà di creare un reato-ostacolo. In tal senso v. *La ratifica della Convenzione Cybercrime*, cit., p. 708.

locuzione espansiva "in qualsiasi modo". Tali condotte sono identiche a quelle sanzionate dall'art. 615-*quater* c.p. Pertanto, per quanto riguarda la critica all'aggiunta della mera detenzione alle condotte sanzionate, si richiama quanto già sostenuto con riferimento a tale ultimo articolo (v. *supra*, par. 3), evidenziando anche in questo caso che l'inserimento della detenzione nulla apporta sul piano della criminalizzazione delle diverse fasi degli attacchi informatici. Anche l'art. 615-*quinquies*, infatti, costituisce norma a più fattispecie, pertanto la progettazione di un programma informatico atto a danneggiare il sistema e la sua successiva vendita nel *dark web* configurerà comunque un unico reato.

Ulteriore modifica di cui alla L. 238/2021 consiste nell'aggiunta dell'avverbio "abusivamente", per cui ora la formulazione della norma ricalca quella di cui all'art. 615-*ter* c.p. Per quanto riguarda il nuovo requisito dell'abusività, in questo caso non si può aderire alla tesi per cui tale richiamo sarebbe pleonastico[147] e si deve invece ritenere che costituisca una clausola d'illiceità speciale[148]. In questo modo, il legislatore ha voluto specificare che la detenzione, la diffusione, l'installazione e tutte le altre condotte descritte sono di per sé lecite, per cui diventano penalmente rilevanti solo se "abusive". Per individuare quando vi sia abusività della condotta tipica, in mancanza di altri riferimenti, nonché in difetto di un inciso analogo a quello di cui all'art. 615-*ter* c.p. sulla mancanza del consenso, si deve fare riferimento al concetto di abusività elaborato con riferimento all'art. 615-*ter* c.p. In particolare, si deve individuare se l'abusività corrisponda soltanto all'assenza di autorizzazione[149], oppure anche alla violazione dei limiti della suddetta valorizzazione[150]. A tal proposito, va rilevato che l'art. 5 della direttiva prevede l'incriminazione delle condotte di interferenza illecita relativamente ai dati a condizione che le stesse siano compiute «*intenzionalmente e senza diritto*», ove il concetto di "senza diritto" viene definito alla lett. d) dell'art. 2 della medesima direttiva come mancanza di autorizzazione da parte del titolare del sistema[151]. In questo caso, dunque, poiché l'intervento legislativo in questione aveva come finalità l'adempimento della direttiva, è proprio la locuzione "senza diritto" quella che costituisce il perno su cui ruota il disvalore del precetto, per cui si ritiene che l'abusività

[147] PICA G., *Diritto penale*, cit., p. 38 ss; GATTA G.L., *Delitti contro l'inviolabilità del domicilio*, cit., p. 353.
[148] SALVADORI I., *I reati contro la riservatezza informatica*, cit., p. 617; *Relazione dell'Ufficio del Massimario presso la Corte di cassazione*, cit., p. 8.
[149] Così FLOR R., *Verso una rivalutazione dell'art. 615-ter c.p.?*, cit., p. 128.
[150] In tal senso SALVADORI I., *Quando un insider accede abusivamente ad un sistema informatico o telematico?*, cit., p. 382.
[151] L'art. 2 lett. d) della Direttiva 2013/40/UE fornisce la seguente definizione di "senza diritto": «*Una condotta di cui alla presente direttiva, ivi inclusi l'accesso, l'interferenza o l'intercettazione, che non è autorizzata da parte del proprietario o da un altro titolare di diritti sul sistema o su una sua parte, ovvero non consentiti a norma del diritto nazionale*».

della condotta coincida con la sola assenza di autorizzazione e non anche con la violazione dei limiti. Non a caso, il nuovo art. 615-*quinquies* c.p., a differenza dell'art. 615-*ter* c.p., menziona solo l'abusività e non anche la mancanza del consenso, a riprova della volontà legislativa di non dilatare eccessivamente l'ambito applicativo della fattispecie.

A seguito delle modifiche introdotte dalla l. n. 48/2008, oggetto del reato sono le apparecchiature, i dispositivi o programmi informatici[152]. È stato eliminato l'inciso che richiedeva che tali oggetti avessero per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione totale o parziale del suo funzionamento, requisito che aveva creato alcuni problemi interpretativi con riferimento alla distinzione tra il danneggiamento e l'interruzione/alterazione del funzionamento[153]. Tali oggetti sono identici ad alcuni di quelli di cui al diverso reato di cui all'art. 615-*quater* c.p. Si discute se nella nozione di programma informatico possano rientrare anche le istruzioni sul modo di creare un programma infetto. Una parte della dottrina ritiene che ciò sia possibile[154], mentre altri, condivisibilmente, evidenziano che le condotte, comunque le si interpretino, hanno ad oggetto specifici strumenti materiali ed immateriali, ovvero dei *software*, non delle mere informazioni[155]. A sostegno di quest'ultima tesi va poi evidenziato che all'art. 615-*quater* c.p. il legislatore ha specificamente previsto di sanzionare coloro che forniscono "indicazioni o istruzioni idonee al predetto scopo", mentre l'art. 615-*quinquies* non contiene analoga previsione. Ciò, dunque, conferma che la fornitura di informazioni o istruzioni idonee alla costruzione di un malware atto a danneggiare i dispositivi informatici non rientra nell'ambito applicativo della fattispecie in esame.

Per quanto riguarda l'elemento soggettivo, a seguito della riforma di cui alla l. 48/2008 è costituito dal dolo specifico[156], per cui occorre che le condotte in questione siano sorrette dal fine specifico di danneggiare illecitamente un sistema informatico o telematico,

---

[152] SALVADORI I., *I reati contro la riservatezza informatica*, cit., p. 703.

[153] In tal senso v. PARODI C., CALICE A., *Responsabilità penali e Internet*, cit., p. 88, nonché PICOTTI L., *La ratifica della Convenzione Cybercrime*, cit., p. 708, il quale evidenzia che con la vecchia formulazione della norma «*si apriva un ampio margine di ambiguità circa i precisi limiti fra lecito ed illecito penale, considerando l'esigenza (e la prassi) di creare sperimentalmente e soprattutto utilizzare programmi di contrasto ai programmi-virus ovvero per aggredire sistemi da cui partano attacchi informatici*».

[154] D'AIETTI G., *La tutela dei programmi e dei sistemi informatici*, in R. Borruso, G. Buonomo, G. Corasaniti, G. D'Aietti (a cura di), *Profili penali dell'informatica*, Milano, 1994, p. 39 ss., p. 89.

[155] PICA G., *Diritto penale delle tecnologie informatiche*, cit., p. 101 s.

[156] Così come prescritto dall'art. 6 co. 2 della Convenzione *Cybercrime*, che espressamente prevede che gli Stati aderenti non devono prevedere una responsabilità penale laddove la produzione, la vendita, l'approvvigionamento per l'uso, l'importazione, la distribuzione o l'utilizzazione in altro modo o il possesso degli oggetti indicati non avvenga allo scopo di commettere un reato in base agli articoli da 2 a 5 della suddetta Convenzione.

le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento. Trattandosi anche in questo caso di condotte c.d. neutre, anche qui il dolo specifico funge da elemento costitutivo dell'illiceità penale. Non solo, perché dato che le condotte coincidono e pure l'oggetto del reato è parzialmente identico, qui il dolo specifico ha anche funzione differenziale rispetto all'art. 615-*quater* c.p.

Nell'ambito applicativo della norma in esame, dunque, rientra l'installazione o comunque la diffusione di un *ransomware*, dato che quest'ultimo *virus* informatico serve proprio ad interrompere il funzionamento del computer. A tal proposito, la giurisprudenza ha ritenuto configurabile il reato in esame in quei casi in cui venga diffuso un virus idoneo ad installarsi abusivamente nel computer della vittima idoneo ad abbassare le misure di sicurezza, atto ad alterare alcune delle funzionalità telematiche dei sistemi informatici[157]. Non vi rientra, invece, l'installazione abusiva di programmi cd. spia quali *Spyware*, *Trojan Horse*, *Keylogger*, ecc., poiché la loro funzione principale è di memorizzare i dati che vengono trattati dall'elaboratore "spiato" e trasmetterli al criminale informatico, senza modificarne il contenuto; dunque, essi non determinano un'alterazione di dati[158].

Analogamente a quanto evidenziato per l'art. 615-*quater* c.p. (v. *supra* par. 3.1), anche per l'art. 615-*quinquies* c.p. si pongono dei problemi con riferimento ai rapporti tra quest'ultima norma e i reati di danneggiamento informatico di cui agli artt. 635-*bis, ter, quater* e *quinquies*. Infatti, le condotte descritte dall'art. 615-*quinquies* c.p., sono prodromiche alla commissione di un danneggiamento informatico. Anche in tal caso, però, non è prevista alcuna clausola di sussidiarietà a favore dei più gravi delitti di danneggiamento. Se si aderisce alla prevalente tesi monista e si utilizza unicamente il criterio della specialità, si deve ritenere che, in caso di avvenuto danneggiamento, tale reato possa concorrere o con il reato di cui all'art. 635-*bis* c.p. in caso di avvenuto danneggiamento di informazioni, dati o programmi informatici altrui (o 635-*ter* c.p., se utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti o comunque di pubblica utilità), o con quello di cui all'art. 635-*quater* c.p. in caso di danneggiamento o ostacolo al funzionamento di sistemi informatici o telematici altrui (o 635-*quinquies* c.p., se utilizzato dallo Stato o da altro ente pubblico o ad essi pertinenti o comunque di pubblica utilità). Nonostante gli artt. 635-*bis, ter* e *quater* c.p. contengano la clausola di sussidiarietà «*salvo che il fatto costituisca più grave reato*», inserita proprio con funzione regolativa "interna" del microsistema dei

[157] Così Tribunale Bologna, sez. I, sentenza 22 dicembre 2005, n. 1823.
[158] SALVADORI I., *Il "microsistema" normativo concernente i danneggiamenti informatici*, cit., p. 209.

danneggiamenti informatici[159], essa non può trovare applicazione nei confronti dell'art. 615-*quinquies*, poiché fattispecie punita meno gravemente. I reati di danneggiamento, inoltre, si consumano in momenti fisiologicamente diversi rispetto a quello di cui all'art. 615-*quinquies* c.p., per cui, secondo il criterio della specialità, si dovrebbe escludere il concorso apparente. Tuttavia, poiché in questo caso si puniscono le diverse fasi dello stesso fenomeno criminoso, con disvalore penale sostanzialmente omogeneo, una duplicazione sanzionatoria automatica non appare corretta. Utilizzando, invece, il diverso criterio di consunzione-assorbimento, possibile anche in ragione dei limiti edittali previsti dalle norme in questione, ben si potrebbe ritenere che l'art. 615-*quinquies* c.p. rimanga assorbito dalla relativa fattispecie di danneggiamento informatico, trattandosi di reato ostacolo rispetto alla realizzazione di offese all'integrità di dati o sistemi informatici[160]. Sussiste però anche qui il problema della diversa procedibilità dei reati, dato che l'art. 615-*quinques* è procedibile d'ufficio, per cui, anche ad accogliere la tesi dell'assorbimento, in caso di rimessione di querela per danneggiamento informatico di cui all'art. 635-*bis* c.p. l'autore del fatto si troverebbe comunque a rispondere del reato prodromico[161].

Dev'essere poi esaminata la possibilità di configurare un concorso tra i delitti di cui agli artt. 615-*quinquies* e 615-*ter* c.p., problema che si è posto con riferimento al caso in cui l'accesso abusivo sia realizzato mediante installazione un *malware* autoreplicante quale il *worm*. Va evidenziato che i beni giuridici tutelati dalle due norme sono diversi, ovvero integrità di dati e sistemi nel primo caso e riservatezza informatica nel secondo, per cui, in mancanza di specialità e data l'eterogeneità delle condotte sanzionate, si deve concludere per la configurabilità del concorso tra le due norme[162]. Per evitare duplicazioni sanzionatorie si dovrebbe considerare l'installazione del programma virus nel computer come antefatto non punibile e applicare così il solo art. 615-*ter* c.p.[163], sanzionato più gravemente, specialmente se considera la presenza della circostanza aggravante di cui all'art. 615-*ter* co. 2 n. 2 c.p. dell'utilizzo della violenza informatica. Infatti, anche se diversi, i beni giuridici tutelati dalle due norme sono comunque sostanzialmente omogenei, dato che, come sopra

[159] CAPPELLINI A., *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici*, cit., p. 795.
[160] In tali termini anche SALVADORI I., *Danneggiamenti informatici*, in *Diritto penale dell'informatica – reati della rete e sulla rete*, a cura di C. Parodi e V. Sellaroli, Milano, 2020, p. 595 ss., p. 621 e CAPPELLINI A., *I delitti contro l'integrità dei dati*, cit., p. 817.
[161] Cft. PAGLIARO A., voce *Concorso di norme penali*, in *Enc. Dir.*, vol. III, Milano, 1961, p. 545 ss., p. 552, che evidenzia che poiché nell'ipotesi della consunzione l'inapplicabilità di una disposizione si verifica in seguito all'assorbimento dello scopo da essa perseguito nello scopo cui tende l'altra norma, la consunzione va esclusa qualora l'interesse di portata maggiore non sia effettivamente tutelato, per cui se il reato più grave non è stato contestato o non è procedibile non si applica alcun assorbimento.
[162] Tesi accolta anche da Corte appello Bologna, sez. II, sentenza 27 marzo 2008 in *Dejure*.
[163] Così anche CAJANI F., *Profili penali del phishing*, in *Cass. pen.*, 2007, n. 6, p. 2294, p. 2298 s.

evidenziato, la riservatezza informatica è essenziale per l'integrità di dati e sistemi. Invece, tra l'art. 615-*quinquies* c.p. e la circostanza aggravante di cui al co. 2 n. 3 dell'art. 615-*ter* c.p., norme caratterizzate dallo stesso disvalore del reato di cui all'art. 615-*quinquies* c.p., ovvero la lesione o la messa in pericolo del bene giuridico dell'integrità di dati o sistemi informatici, vi è un'incompatibilità. Infatti, l'art. 615-*quinquies* c.p. nella sua formulazione attuale è un reato a dolo specifico[164],commesso allo scopo di danneggiare il sistema informatico, mentre, come sopra evidenziato, l'aggravante di cui al n. 3 cit. postula che la distruzione o il danneggiamento siano conseguenza non voluta dell'accesso abusivo. Le due norme, dunque, contrariamente a quanto si riteneva in passato[165], non possono concorrere.

Alcuni autori ritengono poi che il reato in esame possa concorrere anche con la fattispecie di ricettazione di cui all'art. 648 c.p. nei casi in cui il soggetto acquisti il *malware* per distribuirlo sul mercato e in tal modo ricavarne un profitto[166].

7. La rilevanza penale delle intercettazioni informatiche

Con l'art. 6 della citata l. n. 547/1993 il legislatore ha introdotto nella sezione V, dedicata ai «*delitti contro l'inviolabilità dei segreti*», del capo III (delitti contro la libertà individuale) del libro II del codice penale, tre nuove fattispecie, per punire rispettivamente l'intercettazione, l'impedimento o l'interruzione di «comunicazioni informatiche o telematiche» (art. 617-*quater* c.p.), l'installazione di apparecchiature atte ad intercettare, impedire o interrompere le suddette comunicazioni (art. 617-*quinquies* c.p.), nonché la falsificazione, l'alterazione o la soppressione del loro contenuto (art. 617-*sexies* c.p.).

Nel Codice penale italiano la tutela delle comunicazioni telematiche e informatiche è stata costruita simmetricamente rispetto a quella già apprestata negli articoli precedenti per le comunicazioni e conversazioni telefoniche e telegrafiche. L'inserimento nel codice di numerose fattispecie a tutela delle comunicazioni personali, informatiche e telematiche, con conseguente eccessiva frammentazione casistica e duplicazione delle fattispecie incriminatrici è stato oggetto di critiche[167]. In questo modo, infatti, il sistema normativo risulta eccessivamente sovrabbondante. Tuttavia, con l'ultima riforma del 2021 non solo non si è operata quell'auspicata razionalizzazione della materia, ma il problema segnalato è stato addirittura aggravato.

---

[164] PICOTTI L., *La ratifica della Convenzione Cybercrime*, cit., p. 710.
[165] Così Trib. Bologna, sentenza 22 dicembre 2005, n. 1823, in *Giur. merito*, 2006, p. 1224 ss., che fa riferimento all'art. 615-*quinquies* c.p. nella sua vecchia formulazione.
[166] PARODI C., *Profili penali dei virus informatici*, in *Dir. pen. proc*., 2000, n. 5, p. 632 ss., p. 635.
[167] PLANTAMURA V., *La tutela penale delle comunicazioni informatiche e telematiche*, in *Dir. inf. inf.*, 2006, n. 6, p. 847 ss., p. 861.

Anche in questo caso beni giuridici tutelati dalle fattispecie in questione sono la riservatezza e sicurezza informatiche[168], nonostante vi sia chi ritiene che bene giuridico tutelato sia la riservatezza *tout court*, dato che comunque l'elemento principale della tutela resta il carattere personale delle comunicazioni[169]. La giurisprudenza, invece, ritiene che le fattispecie in questione abbiano lo scopo di dare attuazione all'art. 15 Cost., che tutela la libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione[170].

L'art, 617-*quater* c.p. sanziona al co. 1 l'intercettazione, l'interruzione o l'impedimento delle comunicazioni informatiche o telematiche, mentre al co. 2 la loro rivelazione. Per intercettazione si intende la presa di cognizione totale o parziale di una comunicazione[171]. Essa non richiede l'effettiva presa di cognizione del contenuto della comunicazione da parte dell'agente, dato che i sistemi informatici consentono una riproduzione o trasmissione diretta dei dati a terzi, ovvero un loro ulteriore trattamento anche senza alcun diretto intervento dell'uomo o comunque l'apertura dei singoli *files* che li contengono[172]. La norma richiede che l'intercettazione avvenga "fraudolentemente": la fraudolenza va intesa in senso oggettivo, ovvero come modalità occulta di attuazione dell'intercettazione, all'insaputa del soggetto che trasmette la comunicazione[173]. Le altre condotte sanzionate sono l'interruzione, che consiste nel far cessare in qualsiasi modo una comunicazione, e l'impedimento, ovvero l'attività che rende impossibile anche l'inizio della comunicazione relativa al sistema informatico[174]. La rivelazione di cui al co. 2, invece, consiste nell'illegittima divulgazione del contenuto delle comunicazioni informatiche o telematiche e può essere commessa soltanto da colui che ha previamente preso cognizione del contenuto delle comunicazioni[175].

Oggetto di tutela sono soltanto le comunicazioni c.d. chiuse, alle quali si può accedere soltanto violando la loro segretezza della tutela[176]. Ai fini della norma in esame il contenuto delle comunicazioni è irrilevante, per cui oggetto dell'intercettazione possono essere indifferentemente informazioni, notizie e dati[177]. L'elemento soggettivo è il dolo generico, dunque nelle ipotesi di cui al co. 1 è sufficiente la coscienza e volontà di

[168] PICOTTI L. *voce Reati informatici,* cit., p. 6; SALVADORI I., *I reati contro la riservatezza informatica,* cit., p. 706.
[169] PLANTAMURA V., *La tutela penale delle comunicazioni informatiche e telematiche,* cit., p. 861.
[170] Cass. pen., sez. V, sentenza 19 maggio 2005, n. 4011.
[171] PERRI P., *sub art. 617-quater c.p.*, in *Commentario breve al Codice penale,* cit., p. 2148 ss., p. 2149.
[172] PICOTTI L. *voce Reati informatici,* cit., p. 23.
[173] PICA G., *Diritto penale delle tecnologie informatiche,* cit., p. 177.
[174] PERRI P., *sub art. 617-quater c.p.*, cit., p. 2149.
[175] SALVADORI I., *I reati contro la riservatezza informatica,* cit., p. 708.
[176] Cass. pen., sez. V, sentenza 19 maggio 2005, n. 4011.
[177] PERRI P., *sub art. 617-quater c.p.*, cit., p. 2149.

intercettare in modo fraudolento le comunicazioni informatiche o telematiche in fase di trasmissione ovvero di interromperne o impedirne la trasmissione, mentre per quella di cui al co. 2 la coscienza e volontà di rivelare, in tutto o in parte, al pubblico il contenuto di comunicazioni informatiche destinate altrimenti a rimanere riservate[178].

Sono previste delle circostanze aggravanti ad effetto speciale qualora il fatto sia stato commesso in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità, da un pubblico ufficiale o da un incaricato di un pubblico servizio con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema oppure da chi esercita anche abusivamente la professione di investigatore privato. In questi casi è prevista la procedibilità d'ufficio. A seguito della l. 238/2021 sono state aumentate le pene previste sia per la fattispecie base, sia per le ipotesi aggravate. A tal proposito, si evidenzia che la previsione di sanzioni più elevate, prevista per le intercettazioni di comunicazioni informatiche rispetto agli illeciti aventi ad oggetto la corrispondenza informatica o telematica, si giustifica per la necessità di tutelare un interesse super-individuale, ovvero la riservatezza e segretezza delle comunicazioni a prescindere dal loro contenuto[179].

Altra fattispecie prevista è quella di cui all'art. 617-*quinquies* c.p., che punisce le condotte prodromiche all'intercettazione informatica. Trattasi di reato di pericolo, per cui ai fini della sua consumazione non è necessario accertare che i dati siano effettivamente raccolti e memorizzati[180]. Nonostante ciò, in giurisprudenza si ritiene ammissibile la configurabilità del tentativo[181], anche se tale soluzione non appare condivisibile in quanto finisce per anticipare in maniera eccessiva la tutela penale, dato che l'art. 617-*quinquies* c.p. è comunque un reato prodromico alla commissione di ulteriori illeciti[182].

Tale norma è stata oggetto di diverse modifiche da parte della l. 238/2021 cit., a partire dalla sua rubrica, che ora è intitolata «*Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche*». Il novero delle condotte punibili è stato notevolmente ampliato: rispetto all'iniziale sola installazione oggi si sanziona anche colui che «*si procura, detiene,*

[178] SALVADORI I., *I reati contro la riservatezza informatica*, cit., p. 710.
[179] *Ibid*., p. 705 s.
[180] Così Cass. pen., sez. V, sentenza 12 gennaio 2011, n. 6239. In dottrina PERRI P., *sub art. 617-quinquies c.p.*, in *Commentario breve al Codice penale*, cit., p. 2151 ss., p. 2151.
[181] Cass. pen., sez. II, sentenza 9 novembre 2007, n. 45207.
[182] Nello stesso senso anche SALVADORI I., *I reati contro la riservatezza informatica*, cit., p. 714.

produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri». Anche in questo caso la tutela penale è stata notevolmente anticipata e le condotte sanzionate sono identiche a quelle punite dagli artt. 615-*quater* e 615-*quinquies* c.p.

Tra gli oggetti del reato, oltre alle apparecchiature, sono stati aggiunti dalla L. 238/2021 cit. anche programmi, codici, parole chiave o altri mezzi atti ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi. A tal proposito, la giurisprudenza richiede la verifica che le apparecchiature in questione siano idonee a consentire la raccolta o la memorizzazione di dati[183]. Poiché la norma in questione richiede che gli oggetti siano "atti ad intercettare, impedire o interrompere", si ritiene che tale requisito valga anche per i nuovi oggetti del reato ivi elencati.

Le modifiche di cui alla L. 238/2021 cit. rendono questo reato simile all'art. 617-*bis* c.p., a sua volta modificato dalla stessa L. 238/2021, da cui diverge perché questo tutela le comunicazioni e conversazioni telegrafiche o telefoniche, mentre quello di cui all'art. 617-*quinquies* c.p. le comunicazioni informatiche o telematiche[184].

La novella del 2021 è intervenuta anche sull'elemento soggettivo del reato, aggiungendo la locuzione «*al fine di intercettare comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero di impedirle o interromperle*». In questo modo ha posto fine al dibattito dottrinale esistente in merito[185], poiché con l'espressa enunciazione del fine criminoso non vi sono più dubbi sul fatto che l'elemento soggettivo richiesto dall'art. 617-*quinquies* c.p. sia il dolo specifico.

Tra questo reato e quello di cui all'art. 617-*quater* c.p., in mancanza di clausola di sussidiarietà, si pone il problema di individuare se vi è concorso di reati o concorso apparente di norme. Anche in questo caso, applicando il criterio della specialità, si dovrebbe necessariamente concludere che le due fattispecie concorrano tra loro, perché si consumano in momenti differenti[186]. Tuttavia, a ben guardare, non si può che constatare come per intercettare una comunicazione sia necessario quantomeno installare un'"apparecchiatura" che consenta di fare ciò. Per "apparecchiatura", infatti, non si intende solamente un

[183] Cass. pen., sez. V, sentenza 1 febbraio 2016, n. 23604.
[184] PERRI P., *Sub art. 617-quinquies c.p.*, in *Commentario breve al codice penale*, cit., p. 2151 ss., p. 2151.
[185] Secondo un primo orientamento il reato era punito a titolo di dolo generico, poiché non vi era l'enunciazione di alcun fine, v. SALVADORI I., *I reati contro la riservatezza informatica*, cit., p. 714. *Contra* v. PECORELLA C., *Il diritto penale dell'informatica*, Padova, 2006, p. 305.
[186] Favorevole alla tesi del concorso è PERRI P., *Sub art. 617-quater c.p.*, p. 2148 ss., p. 2150.

hardware ma anche un semplice programma informatico di tipo *spyware*[187]. Dunque, è evidente che l'art. 617-*quinquies* c.p. si pone come antecedente necessario rispetto all'art. 617-*quater* c.p. Per questo motivo sarebbe opportuno, anche per evitare duplicazioni sanzionatorie, considerarlo assorbito in quest'ultimo reato[188]. Va però evidenziato che un rilevante ostacolo all'assorbimento è rappresentato dal trattamento sanzionatorio particolarmente elevato dell'art. 617-*quinquies* c.p.

Ultima fattispecie rilevante ai fini dell'analisi in oggetto è quella di cui all'art. 617-*sexies* c.p., che sanziona la falsificazione, l'alterazione o la soppressione del contenuto di comunicazioni informatiche o telematiche. Per quanto riguarda le condotte sanzionate, la falsa formazione di comunicazioni informatiche consiste nella creazione, in tutto o in parte, del contenuto di una comunicazione intercettata, l'alterazione nella modifica totale o parziale del contenuto della comunicazione mediante l'aggiunta, la soppressione o la sostituzione di alcune parti e, infine, la soppressione nella distruzione o eliminazione[189]. Inoltre, è necessario che si realizzi un fatto ulteriore, rappresentato dal farne uso o lasciare che altri ne facciano uso, requisiti da considerarsi elementi del reato e non condizioni obiettive di punibilità[190]. Dunque, il reato si consuma con la effettiva utilizzazione da parte del reo o di un terzo del contenuto delle comunicazioni informatiche intercettate ed oggetto di falsificazione, alterazione o soppressione[191]. Anche in questo caso l'elemento previsto dalla fattispecie è il dolo specifico, che consiste nel fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno.

Le tre fattispecie sopra menzionate possono trovare applicazione durante le diverse fasi di un attacco informatico contro il patrimonio. Infatti, per riuscire a carpire da remoto i dati personali o le credenziali altrui allo scopo di effettuare un accesso abusivo finalizzato ad una frode informatica, qualora non sia la vittima stessa a fornirle al criminale perché tratta in inganno dai messaggi di *phishing*, è necessaria la previa installazione di un programma *virus* nel computer della vittima, che intercetti i dati in entrata o in uscita e dunque anche le sue *password*. Tale condotta è astrattamente riconducibile non solo al reato di cui all'art. 617-*quater* c.p., ma anche a quello di cui all'art. 617-*quinquies* c.p., come ritenuto dalla stessa giurisprudenza della Cassazione[192]. Come sopra evidenziato, le due norme

[187] SALVADORI I., *I reati contro la riservatezza informatica*, cit., p. 713.
[188] In tal senso anche Cass. pen., sez. V, sentenza 29 gennaio 2016, n. 4059, che evidenzia come si tratti di una progressione criminosa.
[189] SALVADORI I., *I reati contro la riservatezza informatica*, cit., p. 716.
[190] PERRI P., *Sub art. 617-sexies c.p.*, in *Commentario breve al codice penale*, cit., p. 2151 ss., p. 2152.
[191] SALVADORI I., *I reati contro la riservatezza informatica*, cit., p. 718.
[192] Cass. pen., sez. II, sentenza 9 novembre 2007, n. 45207.

menzionate, infatti, non descrivono quale debba essere il contenuto della comunicazione, per cui oggetto dell'intercettazione possono anche essere informazioni, notizie e dati, dunque anche i codici alfanumerici di accesso degli utenti[193].

Ciò posto, si pone il problema della configurabilità o meno del concorso tra tali reati e gli altri reati sopra descritti, in particolare tra l'accesso abusivo a sistema informatico o telematico e la frode informatica. Sul punto, la giurisprudenza ha ritenuto che il delitto di cui all'art. 617-*quater* c.p. e quello di frode informatica possano concorrere tra loro, in ragione della diversità dei beni giuridici tutelati e delle condotte sanzionate, dato che la prima fattispecie è diretta a garantire la libertà e la segretezza delle comunicazioni telematiche, mentre la frode informatica contempla l'alterazione dei dati immagazzinati nel sistema al fine della percezione di ingiusto profitto e nasce con la *ratio* di offrire tutela al patrimonio[194]. Effettivamente i due reati si consumano in momenti differenti, per cui non possono essere tra loro in rapporto di specialità e si deve necessariamente concludere per il concorso. Va però evidenziato che vi è pur sempre l'aggravante di cui all'art. 640-*ter* co. 3 c.p. della frode informatica commessa con furto o indebito utilizzo di identità digitale (v. infra cap. III, par. 2.1). Infatti, poiché per "rubare" le credenziali altrui è necessario intercettare i dati sul computer della vittima, dato che non le si possiede già, le condotte sanzionate vengono a coincidere. Si può dunque ritenere che l'art. 640-*ter* co. 3 c.p., proprio perché circostanza aggravante che accede ad una frode informatica, sia speciale rispetto all'art. 617-*quater* c.p. e che, dunque, si applichi solo la prima delle due fattispecie, che, peraltro, può essere considerata anche come reato complesso, dato che l'intercettazione fraudolenta dei dati di accesso al *computer* altrui può considerarsi elemento costitutivo della frode informatica aggravata dal furto d'identità digitale. A tale tesi ha recentemente aderito anche la Cassazione, ritenendo il reato di cui all'art. 617-*quater* c.p. assorbito nella frode informatica[195].

Per quanto riguarda, invece, la configurabilità del concorso tra l'intercettazione illecita di comunicazioni informatiche o telematiche ex art. 617-*quater* c.p. e gli artt. 615-*quater* e 615-*ter* c.p., va evidenziato che l'intercettazione delle credenziali altrui si pone in

[193] Così Cass. pen., sez. II, 9 novembre 2007, n. 45207 secondo cui «*Integra la condotta di "intercettazione", rilevante ai sensi dell'art. 617 quater c.p., la condotta di colui che utilizza apparecchiature idonee a copiare degli i codici alfanumerici di accesso utenti, mediante applicazione ai terminali automatici delle banche. La digitazione del codice di accesso costituisce, invero, la prima comunicazione dell'utente con il sistema informatico, con la conseguenza che la copiatura di detti codici rientra nel concetto di intercettazione di comunicazioni telematiche preso in considerazione dalla citata disposizione normativa*»; nello stesso senso anche Cass. pen., sez. V, 30 gennaio 2007, n. 3252.
[194] Così Cass. pen., Sez. V, sentenza 9 ottobre 2020, n. 869.
[195] Cass. pen., sez. V, 7 settembre 2021, n. 42183.

rapporto di stretta consequenzialità con il reato di accesso abusivo a sistema informatico o telematico e può coincidere con la condotta di "procurarsi" codici d'accesso a sistemi informatici o telematici. A tal proposito, la giurisprudenza di legittimità ha ritenuto configurabile il concorso tra il reato di cui all'art. 617-*quater* c.p. e quello di accesso abusivo a sistema informatico o telematico[196]. Anche in questo caso i due reati si consumano in momenti diversi e le condotte sanzionate sono eterogenee tra loro, per cui anche qui, non potendosi ravvisare alcun rapporto di specialità, si deve necessariamente ritenere configurabile il concorso. Il discorso è più complesso per quanto riguarda il rapporto con l'art. 615-*quater* c.p., dato che le condotte sanzionate possono coincidere: infatti, è ben possibile procurarsi le *password* di accesso previa installazione di uno *spyware* nel computer della vittima. In questo caso, dunque, l'intercettazione di dati diventa una modalità di commissione del reato di cui all'art. 615-*quater* c.p. e si può ritenere che sia applicabile soltanto quest'ultima. Nel caso di avvenuto accesso abusivo, però, poiché gli artt. 617-*quater* e 615-*quater* c.p. si pongono come antecedenti necessari, sarebbe più opportuno considerare l'intercettazione di dati come antefatto non punibile e applicare solamente la fattispecie di accesso abusivo a sistema informatico o telematico, valorizzando la finalità dell'intercettazione. A tal proposito, si evidenzia che il bene giuridico tutelato è sostanzialmente omogeneo, ovvero la riservatezza informatica, intesa come interesse al godimento e controllo esclusivi dei prodotti e dell'utilità delle nuove tecnologie[197].

Il problema del concorso si pone anche con l'art. 617-*sexies* c.p., dato che la giurisprudenza di merito ha ritenuto che l'invio di *mail* di *phishing* sia condotta idonea ad integrare il reato in esame[198], trattandosi di falsa comunicazione. A tal proposito, la stessa giurisprudenza ha ritenuto che il reato in questione possa concorrere con il reato di cui all'art. 615-*ter* c.p., data la diversità delle condotte sanzionate dalle due norme, soluzione con la quale, in base al principio di specialità, non si può che concordare.

Il problema del concorso si pone anche con riferimento al reato di cui all'art. 493-*ter* c.p., ovvero di indebito utilizzo di carte di credito oppure di falsificazione o alterazione di carte di credito, dato che, come esaminato in precedenza, oggetto materiale dell'intercettazione possono essere anche i codici o i numeri delle carte di credito[199]. In passato, infatti, la Cassazione ha ritenuto applicabile il reato di cui all'art. 617-*quater* c.p.

[196] Cass. pen., sez. II, sentenza 17 giugno 2019, n. 26604.
[197] PICOTTI L., *Sistematica*, cit., p. 76 s.
[198] Tribunale Milano, sez. uff. gip., 10/12/2007.
[199] Cass. pen., sez. II, 9 novembre 2007, n. 45207, cit. e Cass. pen., sez. V, 30 gennaio 2007, n. 3252, cit.

anche all'utilizzo di carte di credito clonate[200], mentre l'art. 617-*quinquies* c.p. all'installazione di uno *skimmer* per intercettare i codici delle carte di credito[201]. Anche in questo caso va esclusa la sussistenza di un rapporto di specialità tra l'art. 617-*quater* c.p. e le fattispecie di indebito utilizzo, falsificazione o alterazione di carte di credito, perché le condotte sanzionate sono eterogenee e i reati si consumano in momenti differenti, dato che l'intercettazione viene effettuata proprio allo scopo di poter carpire i dati della carta di credito altrui. Tuttavia, anche in questi casi non si può trascurare come i reati siano tra loro in rapporto di stretta consequenzialità, dato che l'intercettazione è il mezzo con cui il reo riesce a procurarsi i dati delle carte di credito per poi realizzarne di clonate e usarle per fare acquisti o prelievi indebiti. Si può, dunque, ritenere che anche in questo caso vi sia una vera e propria progressione criminosa e concludere per l'applicabilità del solo art. 493-*ter* c.p. Il problema, invece, non si pone per il diverso reato prodromico all'indebito utilizzo di carte di credito di cui all'art. 493-*quater* c.p., data la clausola di sussidiarietà presente in quest'ultima fattispecie e le pene più elevate previste per i reati di cui agli artt. 617-*quater* e 617-*quinquies* c.p.

Infine, non si può trascurare che gli attacchi *man-in-the-middle*, nei quali il criminale informatico intercetta i messaggi indirizzati ad un sito o un indirizzo *mail* scelto da un qualsiasi utilizzatore, salva le informazioni che gli interessano, poi ritrasmette i messaggi al sito scelto dalla vittima ed infine le inoltra le risposte di ritorno, possono astrattamente configurare anche la fattispecie di cui l'art. 617-*sexies* c.p., che punisce la falsificazione, l'alterazione o la soppressione del contenuto di comunicazioni informatiche o telematiche. In particolare, l'inoltro delle risposte artefatte da parte del criminale informatico può configurare la falsificazione, o comunque l'alterazione del contenuto di comunicazioni informatiche, dato che può costituire falsificazione la creazione in tutto o in parte del contenuto di una comunicazione intercettata[202]. Si pone, dunque, il problema della configurabilità del concorso col reato di frode informatica, dato che gli attacchi di questo tipo sono per la gran parte finalizzati proprio alla commissione di tale ultimo reato. Anche in questo caso, analogamente a quanto sopra esposto per il reato di cui all'art. 617-*quater*

[200] Cass. pen., sez. V, sentenza 14 ottobre 2003, n. 44362. Tale tesi è stata criticata da ATERNO S., *La Cassazione non convince sull'intercettazione illecita di comunicazioni informatiche e telematiche*, in *Cass. pen*., 2005, n. 5, p. 1582 ss., p. 1582 ss., il quale sostiene la sola applicabilità delle fattispecie in materia di carte di credito, oggi strumenti di pagamento diversi dai contanti.
[201] Cass. pen., sez. V, sentenza 12 gennaio 2011, n. 6239 e Cass. pen., sez. V, sentenza 9 luglio 2010, n. 36601. In senso difforme v. Cass. pen., sez. V, sentenza 22 novembre 2019, n. 3236, secondo cui tale fattispecie non sarebbe configurabile nel caso in esame perché lo skimmer non è apparecchio idoneo a riprendere i codici Pin dei clienti.
[202] SALVADORI I., *I reati contro la riservatezza informatica*, cit., p. 716.

c.p., si può concludere per la sola applicabilità della frode informatica ex art. 640-*ter* c.p. co. 3, aggravata dall'indebito utilizzo dell'identità digitale altrui, evitando così duplicazioni sanzionatorie.

8. La sostituzione di persona

Altra fattispecie che viene in evidenza nella fase prodromica all'effettiva commissione di un reato contro il patrimonio è quella di cui all'art. 494 c.p., che punisce la sostituzione di persona. Tale fattispecie assume particolare rilievo, poiché, come osservato, in moltissimi casi i criminali informatici assumono identità fittizie o di ignari utenti per ingannare le loro vittime e andare esenti da responsabilità penale. Si può, invece, anche in ragione della clausola di sussidiarietà contenuta in detta norma, escludere l'applicabilità di altri delitti contro la fede pubblica, ovvero i delitti di falso. Questo perché tali *e-mail* fasulle non possono che essere qualificate come scrittura privata, la cui falsificazione è stata depenalizzata dal d.lgs. 15 gennaio 2016[203].

Il bene giuridico tutelato dalla norma è quello della fede pubblica, da proteggere da quei comportamenti che alterano gli elementi di identificazione personale di un soggetto oppure le qualità che ne condizionano il ruolo nella società civile[204], anche se oggi si riconosce la natura plurioffensiva del delitto, in quanto è preordinato non soltanto alla tutela di un interesse pubblico, ma anche a quella del soggetto privato cui l'atto sia destinato ad incidere[205]. L'oggetto giuridico tutelato da questa fattispecie consiste dunque nell'obbligo di farsi conoscere per quello che si è, in modo da non ledere la pubblica fede con dichiarazioni false in strumenti di identificazione[206].

La condotta tipica consiste nell'induzione in errore ovvero nel provocare in taluno una falsa rappresentazione della realtà[207]. Trattandosi di fattispecie a forma vincolata, l'azione per essere penalmente rilevante deve assumere una delle quattro forme previste dalla norma, ovvero: la sostituzione illegittima della propria ad altrui persona, l'attribuzione a sé o ad altri di un falso nome (ossia il complesso dei requisiti di identità di un soggetto, quali il luogo, data di nascita, paternità e maternità, ecc.), di un falso stato (condizione della

[203] CAJANI F., *Profili penali del phishing,* in *Cass. pen.*, n. 6, 2007, p. 2294 ss., p. 2295.
[204] FIANDACA G., MUSCO E., *Dir. pen., PS,* vol. I, V ed., Bologna, 2012, p. 619.
[205] In giurisprudenza v. *ex multis* Cass pen., sez. V, 27 marzo 2009, n. 21574. In tal senso in dottrina anche MARRAFFINO M., *La sostituzione di persona mediante furto d'identità digitale*, in *Cybercrime*, cit., p. 307 ss., p. 311.
[206] ASTORINA MARINO P., *Sub art. 494 c.p.,* in *Commentario breve al codice penale*, cit., p. 1652 ss., p. 1652; CRISTANI A., voce *Falsità personale*, in *Dig. disc. pen.*, vol. V, Torino, 1991, p. 107 ss., p. 107; PAGLIARO A., voce *Falsità personale*, in *Enc. dir.*, XVI, Milano, 1967, p. 646 ss., p. 646 ss.
[207] ASTORINA MARINO P., *Sub art. 494 c.p.*, cit., p. 1653.

persona nella società, cittadinanza, capacità di agire, stato civile, parentela e affinità, ecc.) o di una qualità cui la legge attribuisca effetti giuridici, quali, ad esempio, le qualifiche di proprietario, possessore, creditore, età, qualifica professionale o attribuzione sociale. Il reato è punito a titolo di dolo specifico perché è richiesto che il fatto-base della sostituzione di persona venga compiuto al fine di procurare a sé o ad altri un vantaggio o di procurare un danno, vantaggio che non è da confondere con la nozione di lucro, perché in questo caso non rilevano finalità esclusivamente pecuniarie, ma l'utilità che si intende perseguire può riguardare qualsiasi aspetto personale o della vita di relazione[208].

Una parte della dottrina ha evidenziato le difficoltà di applicazione del delitto di sostituzione di persona al fenomeno del *phishing*[209]. Innanzitutto, l'invio di un'*e-mail* che imiti pagine *web* e siti di mittenti reali non implica che il riferimento sia indicativo o distintivo di un mittente persona fisica. Anzi, spesso i messaggi fanno riferimento a persone giuridiche, quali istituzioni pubbliche o istituti di credito; quindi, non si tratterebbe propriamente di "sostituzione" materiale della propria all'altrui persona fisica. Inoltre, secondo questa tesi, l'utilizzo *online* degli estremi identificativi di una persona reale, quali le credenziali di autenticazione per l'accesso a sistemi informatici o spazi virtuali esclusivi, non corrisponderebbe all'attribuzione illecita di un falso nome, di un falso stato o di una qualità a cui la legge riconosce effetti giuridici. Nel *phishing*, infatti, rileva l'utilizzo non autorizzato dei dati legati ad un soggetto, che lo identificano virtualmente nelle sole operazioni di accesso o di connessione al sistema informatizzato. Secondo tale orientamento non verrebbe dunque in considerazione il bene della conoscenza certa della persona o delle sue qualità essenziali, così come non vi sarebbe una materiale sostituzione della persona fisica. La giurisprudenza di legittimità, invero, interpreta estensivamente gli elementi oggettivi di tale reato, che ha ritenuto applicabile in numerose occasioni anche alla creazione di un *account* di posta elettronica riferibile ad altra persona o all'utilizzo di un *nickname* riconducibile ad altro soggetto assieme all'inserimento del numero telefonico di quest'ultimo su un sito di incontri[210], evidenziando che il reato in questione può essere integrato anche dall'assunzione di un nome immaginario[211].

Tuttavia, anche ad ammettere tale interpretazione estensiva, secondo tali autori per

[208] *Ibid*., p. 1654.
[209] FLOR R., *Phishing, identity theft,* cit., p. 902 s.
[210] Così Cass. 15 dicembre 2011, n. 12479, Cass. 8 novembre 2007, n. 46674 in Dir. inf. inf., 2008, 525 ss. e Cass. 28 novembre 2012, n. 18826 in *Dir. pen. cont*., 25 giugno 2013, disponibile *online* all'indirizzo www.penalecontemporaneo.it con nota di GIUDICI A., *Creazione di un falso profilo utente sulla rete e delitto di sostituzione di persona*.
[211] V. Cass., 21 dicembre 2011, n. 4250 e Cass. 27 settembre 2006, n. 36094

l'applicazione della fattispecie rimarrebbe in ogni caso l'ostacolo insuperabile costituito dall'evento, ovvero l'induzione in errore. Quest'ultimo elemento, infatti, non sarebbe in alcun modo compatibile o applicabile all'esecuzione automatizzata di richieste inoltrate ai sistemi informatici. Si aggiunga poi che l'inserimento *online* dei dati o delle credenziali di autenticazione di un altro soggetto da parte dell'agente non è condotta idonea a trarre in inganno il sistema informatico, perché quest'ultimo esegue unicamente e fedelmente le istruzioni impartite dalla persona fisica, la quale, per la macchina, corrisponde sempre a quella legittimata, proprio perché ne utilizza l'identità virtuale[212]. Diverso discorso potrebbe farsi in casi di *Vishing*, nel quale il destinatario del messaggio viene invitato ad attivare una chiamata *Voice over IP* ad un *call center* apparentemente riconducibile ad un'istituzione reale, perché in tal caso si realizza la falsa attribuzione di una qualità, che permette di poter richiedere informazioni riservate, creando al contempo nell'utente interlocutore telefonico una erronea situazione di affidamento nell'attività propria dell'istituzione reale[213]. Anche seguendo tale prospettazione, però, se alla chiamata abbia risposto una voce elettronica registrata non vi sarebbe stato contatto diretto, per cui il fatto non potrebbe comunque essere ricondotto nell'ambito applicativo della fattispecie delittuosa in esame[214].

Tale tesi non è stata accolta dalla giurisprudenza di merito, che ritiene che la prima fase dei *phishing attacks* sia punibile ai sensi dell'art. 494 c.p.[215], evidenziando che l'induzione in errore rilevante è quella della vittima, ingannata in merito all'autenticità del messaggio ricevuto e stimolata così a fornire i propri dati[216]. Effettivamente in questi casi vi è un'effettiva induzione in errore del soggetto passivo, mentre l'inserimento online dei dati o delle credenziali di autenticazione di quest'ultimo illecitamente carpite è condotta successiva, che viene commessa quando la sostituzione di persona si è già consumata. L'induzione in errore non deve essere riferita al sistema informatico, per cui non appaiono esservi ostacoli rilevanti all'applicazione della norma in questione anche al fenomeno del *phishing*. Si pongono, però, problemi con riferimento ai rapporti tra tale fattispecie e la circostanza aggravante della frode informatica di cui all'art. 640-*ter* co. 3 c.p. del fatto commesso con furto o indebito utilizzo dell'identità digitale, che saranno analizzati nel prossimo capitolo (v. *infra* cap. III, par. 2.1).

---

[212] *Ibid*.
[213] FLOR R., *Phishing, identity theft,* cit., p. 903.
[214] in questi termini PERRI P., *Lo smishing e il vishing,* cit., p. 267.
[215] Così Trib. Milano, Ufficio G.I.P., 29 ottobre 2008, n. 8542, in *Cor. mer.*, 2009, n. 3, p. 285 ss.; Trib. Milano, 7 ottobre 2011, in *Dir. pen proc*., n.1, 2012, p. 55
[216] Per la dottrina così anche CAJANI F., *Profili penali del phishing*, cit., p. 2295.

Non sussistono dubbi, invece, sull'applicabilità della norma in questione nei casi di *advance fee fraud* o comunque di truffe *online* qualora il reo utilizzi indebitamente il nome, l'immagine, il logo, ecc. di una persona realmente esistente ignara al fine di ingannare le sue vittime o comunque un nome di fantasia[217]. La giurisprudenza, infatti, a fronte del proliferare della creazione sui *social network* di identità fittizie o multiple per scopi illeciti e in mancanza di interventi legislativi sistematici idonei ad adeguare il diritto penale ai cambiamenti sociali, si è avvalsa dello strumento dell'interpretazione estensiva[218]. Pertanto, ha in più occasioni ritenuto applicabile tale fattispecie anche a condotte illecite poste in essere nel *web*[219], quali la creazione di un *account* di posta elettronica riferibile ad altra persona[220] o l'utilizzo di un *nickname* riconducibile ad altro soggetto assieme all'inserimento del numero telefonico di quest'ultimo su un sito di incontri[221]. Tale operazione ermeneutica è possibile perché le falsità personali sono caratterizzate dal contenuto della rappresentazione e non dalla forma[222]: non si fa riferimento alla persona fisica in sé, bensì all'identità e alle altre qualità della persona. Infatti, oggetto di tutela della norma è la corrispondenza alla realtà dei fatti di dichiarazioni che si riferiscono all'identità o a qualità personali della persona, che finiscono per creare un'aspettativa di verità e corrispondenza rispetto a quelle reali del soggetto. Dunque, poiché anche l'effigie di una persona costituisce dato personale che ne consente la diretta identificazione[223], colui che utilizza una fotografia altrui fingendo di essere la persona ivi ritratta sostituisce illegittimamente la propria all'altrui persona. Anche il semplice utilizzo di una fotografia altrui, quindi, è sufficiente ad integrare il reato di sostituzione di persona, mentre non rileva che alla foto profilo sia associato un

[217] Cass. pen., sez. II, sentenza 21 dicembre 2011, n. 4250.
[218] In base a tale criterio ermeneutico viene attribuito il più ampio significato tra quelli possibili agli elementi tipici che compongono la fattispecie, al contrario invece di quanto accade per l'analogia, ove si travalicano i confini della norma penale perché il caso di cui trattasi non può essere in alcun modo ricompreso nella stessa neanche se interpretata nella sua massima estensione. Sulla differenza tra analogia e interpretazione estensiva vedi, per tutti, MANTOVANI F., *Dir. pen., PG*, X ed., Padova, 2017, p. 73. In giurisprudenza v. Cass. 27 aprile 1990, n. 11380.
[219] Cft. Cass. 8 giugno 2018, n. 33862 e Cass. 23 aprile 2014, n. 25774 con nota di SANSOBRINO F., *Creazione di un falso account, abusivo utilizzo dell'immagine di una terza persona e delitto di sostituzione di persona*, in *Dir. pen. cont.*, 30 settembre 2014, disponibile *online* all'indirizzo http://www.penalecontemporaneo.it.
[220] Così Cass. 15 dicembre 2011, n. 12479 e Cass. 8 novembre 2007, n. 46674 in *Dir. inf. inf*., 2008, 525 ss.
[221] Cass. 28 novembre 2012, n. 18826.
[222] CRISTANI A., voce *Falsità personale*, cit., p. 107; FLICK C., *Falsa identità su internet e tutela penale della fede pubblica degli utenti e della persona*, in *Dir. inf. inf.*, 2008, n. 4-5, p. 526 ss., p. 536.
[223] In tal senso depone l'art. 4 del regolamento europeo 2016/679 UE, secondo cui per dato personale si intende «*qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*».

nome di fantasia o di persona inesistente. Infatti, il reato in esame, anche se è a forma vincolata[224], può realizzarsi alternativamente secondo una delle quattro modalità contemplate, ovvero la sostituzione illegittima della propria all'altrui persona o l'attribuzione a sé o ad altri di un falso nome, di un falso stato o di una qualità cui la legge riconnette effetti giuridici[225]. Si tratta, quindi, di norma a più fattispecie, la cui eventuale compresenza di più tra le modalità descritte non dà vita a pluralità di reati[226].

9. Le norme incriminatrici contenute nel c.d. codice della *privacy*

Come evidenziato in precedenza, le nuove modalità di aggressione al patrimonio non ledono unicamente la riservatezza informatica, ma anche il diritto alla tutela dei dati personali.

In passato vi era chi aveva ipotizzato l'applicabilità alla seconda fase dei *phishing attacks* della fattispecie di cui all'art. 167 d.lgs. 30 giugno 2003 n. 196 (c.d. codice *privacy*), rubricato "*trattamento illecito di dati personali*", che puniva la violazione dell'art. 23 d.lgs. cit., ovvero il trattamento di dati personali avvenuto senza consenso dell'interessato[227]. In particolare, si era evidenziato che la raccolta di dati, codici d'accesso, *password*, ecc. effettuata dal *phisher* era idonea ad essere ricompresa nella nozione di trattamento, così come numeri di conti correnti e di carte di credito o di pagamento, *passwords*, credenziali, ecc. alla nozione di "dati personali", trattandosi di informazioni relative ad una persona fisica riconducibili all'identificazione. Non è mancata giurisprudenza che ha ritenuto applicabile il reato di trattamento illecito di dati personali nel caso in cui il reo abbia inserito in *chat* il numero di utenza cellulare di un'altra persona, qualificando quest'ultimo come dato personale[228].

Si poneva, dunque, un problema di concorso con le fattispecie già esaminate di accesso abusivo a sistema informatico o telematico, detenzione e diffusione abusiva di codici d'accesso nonché con la stessa frode informatica. Escludendo un rapporto di specialità, la giurisprudenza ha ritenuto configurabile il concorso tra la fattispecie di illecito trattamento dei dati personali e quella di cui all'art. 615-*ter* c.p., riscontrando «*una diversità di condotte*

[224] FIANDACA G., MUSCO E., *Dir. pen., PS*, cit., p. 619.
[225] ASTORINA MARINO P., *Sub art. 494 c.p.*, cit., p. 1653.
[226] PAGLIARO A., voce *Falsità personale*, cit., p. 646 ss.
[227] FLOR R., *phishing, identity theft,* cit., p. 908.
[228] V. Cass. pen., sez. III penale, sentenza 14 novembre 2019, n. 46376 e Cass. pen., sez. III penale, sentenza 17 febbraio 2011, n. 21839

finalistiche e una diversità di attività materiali che non lascia sussistere tra esse quella relazione di omogeneità che le rende riconducibili "ad unum" nella figura del reato speciale ex art. 15 c.p.»[229]. A tal proposito, se si utilizzazze il criterio della specialità, non vi sarebbe nulla da eccepire, dato che effettivamente i due reati si consumano in momenti fisiologicamente diversi. Tuttavia, è stato evidenziato che l'illecito trattamento di dati personali è finalizzato proprio alla commissione di un accesso abusivo al sistema informatico, per cui, forse, sarebbe stato più opportuno considerare il primo come antefatto nell'ambito di una progressione criminosa. Il rapporto di specialità, invece, poteva invece essere ritenuto sussistente col diverso reato di detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici, in ragione dell'identità dell'elemento soggettivo nonché dell'omogeneità delle condotte sanzionate, eterogenee soltanto in apparenza. Infatti, come sopra evidenziato, la raccolta di dati (riconducibile alle condotte di "procurarsi, diffondere o comunicare" di cui all'art. 615-*quater* c.p.) veniva ricompresa nella nozione di trattamento, mentre le *password*, credenziali, ecc. potevano essere riconducibili sia alla nozione di "dati personali", trattandosi di informazioni relative ad una persona fisica che ne consentono l'identificazione, sia a quella di mezzi idonei all'accesso ad un sistema informatico, oggetti materiali del reato di cui all'art. 615-*quater* c.p. In questo caso, qualora i dati personali fossero stati anche idonei all'accesso al sistema informatico o telematico, si sarebbe potuto valorizzare il profilo relativo alla raccolta ai fini dell'accesso e ritenere speciale il reato di cui all'art. 615-*quater* c.p. A ben guardare, però, le due fattispecie apparivano più in rapporto di specialità bilaterale per aggiunta, data la diversità degli elementi presenti nelle diverse norme, per cui in tal caso si sarebbe dovuto ritenere sussistente il concorso tra le due fattispecie.

Meno problematico invece era il rapporto con la frode informatica, per via della presenza della clausola di sussidiarietà presente nel reato di trattamento illecito di dati personali, per cui, essendo il trattamento illecito di dati personali punito meno severamente rispetto alla frode informatica, si poteva ritenere quest'ultimo sussidiario rispetto al primo.

Oggi però il quadro normativo è mutato. Infatti, tale fattispecie è stata modificata dall'art. 15, co. 1, lett. b) del d.lgs. 10 agosto 2018, n. 101, di adeguamento del c.d. codice *privacy* alle disposizioni del Regolamento 2016/679/UE o GDPR, ed è stato eliminato il riferimento alla violazione dell'art. 23 d.lgs. 196/2003, relativo alla prestazione del consenso

[229] Cass. pen., sez. V, sentenza 13 marzo 2017, n. 11994. Più di recente nello stesso senso anche Cass. pen., sez. V, sentenza 4 ottobre 2021, n. 1761.

al trattamento dei dati personali, che è stato contestualmente abrogato e sostituito dall'art. 6 del Regolamento 2016/679/UE sulle condizioni di liceità del trattamento dei dati personali[230]. Il co. 1 del modificato art. 167, dunque, fa riferimento soltanto alla violazione delle disposizioni di cui agli artt. 123 (dati relativi al traffico), 126 (dati relativi all'ubicazione), 130 (comunicazioni indesiderate) e 129 (dati personali relativi ai contraenti negli elenchi cartacei o elettronici a disposizione del pubblico) del d.lgs. 196/2003. Pertanto, poiché la condotta del *phisher* non si sostanzia nella violazione di nessuna di queste disposizioni, la fattispecie in questione non è più applicabile. La "pesca" fraudolenta di codici d'accesso, inoltre, non è ricompresa neppure tra le condotte sanzionate dal successivo co. 2 dell'art. 167 di nuova formulazione, poiché in tale disposizione si fa riferimento ai "*dati personali di cui agli articoli 9 e 10 del Regolamento*" [231] e le credenziali di autenticazione e le *password* non possono essere ricondotte a tali categorie di dati. Dunque, a causa di questa parziale *abolitio criminis*, si può ritenere in parte risolto anche il problema relativo all'eventuale concorso di reati. Tuttavia, nel caso in cui il sistema di autentificazione funzioni tramite impronta digitale o simili, trattandosi di "dato biometrico" di cui all'art. 9 del Regolamento 2016/679/UE, la fattispecie di trattamento illecito di dati personali è tuttora applicabile. In questi casi, dunque, con riferimento ai rapporti con le altre fattispecie, si può ritenere valido quanto sopra esposto in riferimento alla formulazione del vecchio art. 167 d.lgs. 196/2003. Inoltre, in caso di acquisizione di un archivio informatizzato contenente *password* e codici d'accesso degli utenti, potrà essere integrato il nuovo reato di cui all'art. 167-*ter* d.lgs. 196/2003, introdotto dal d.lgs. 101/2018, che punisce l'acquisizione fraudolenta di dati personali su larga scala. Se, poi, il *phisher* comunica o diffonde tali dati, commetterà il diverso reato di cui all'art. 167-*bis* d.lgs. 196/2003, che punisce la comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala, fattispecie che prevale sull'art. 167-*ter* in ragione della clausola di sussidiarietà presente in tale ultima norma, punita meno severamente[232].

In questo caso, con riferimento al reato di cui all'art. 615-*quater* c.p., al contrario di quanto evidenziato per il diverso reato di cui all'art. 167 codice *privacy*, l'art. 167-*bis* codice

---

[230] Per una panoramica delle modifiche apportate all'impianto sanzionatorio del codice *privacy* dal d.lgs. 101/2018 cit. v. DEL NINNO A., *Il nuovo impianto sanzionatorio penale del Codice della privacy coordinato al GDPR. Le principali novità in materia di reati privacy*, in *Dir. & Giust.*, 2018, p. 1 ss.

[231] Ovvero i «*dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona*» e i «*dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1*»

[232] RESTA F., *I reati in materia di protezione dei dati personali*, in *Cybercrime*, cit., p. 1019 ss., p. 1036 ss.

privacy può considerarsi norma speciale in ragione della peculiarità dell'oggetto materiale del reato, ovvero un intero archivio e non semplici dati personali idonei all'accesso al computer. Analoga considerazione vale anche per l'art. 167-*ter* codice *privacy*, il quale, inoltre, richiede anche che l'acquisizione avvenga con mezzi fraudolenti, ulteriore elemento non previsto dall'art. 615-*quater* c.p.

10. La controversa rilevanza penale del c.d. furto di dati e della c.d. ricettazione di dati

Il quadro dei rapporti tra le diverse fattispecie è ulteriormente influenzato dalla recentemente giurisprudenza della Suprema Corte, che recentemente ha affermato che i dati possono essere ricompresi del concetto di "cosa mobile" ai fini del diritto penale[233]. La Cassazione, infatti, ne ha ritenuto sussistente la fisicità in quanto misurabili in *bit* e *byte* e perciò possibile oggetto di operazioni di trasferimento o custodia, elementi che rappresenterebbero i presupposti logici della possibilità che il dato informatico sia oggetto di condotte di sottrazione e appropriazione. Quest'interpretazione, peraltro non da tutti condivisa[234] perché in violazione del divieto di analogia *in malam partem*, apre le porte alla configurabilità del reato di furto avente quale oggetto materiale i dati o i programmi informatici[235], con applicazione delle elevate pene ivi previste.

Tale orientamento rappresenta una rottura rilevante rispetto al passato. In precedenza, infatti, la giurisprudenza escludeva la configurabilità del "furto" o dell'appropriazione indebita di dati per impossibilità di ricondurre la nozione di dati al concetto di "cosa mobile" e riteneva potesse essere rubato unicamente il supporto ove i dati erano memorizzati o comunque l'entità materiale su cui tali dati erano stati trasfusi ed incorporati attraverso la stampa del contenuto[236].

Questa nuova interpretazione del concetto di "cosa mobile" pone anche il problema di stabilire se tale fattispecie possa o meno concorrere con le altre già esaminate in precedenza, in particolare con l'accesso abusivo a sistema informatico, la detenzione e diffusione abusiva di codici d'accesso a sistemi informatici o telematici e la frode

[233] Cass. pen., sez. II, 10 aprile 2020, n. 11959 con nota di CASTAGNO J.P., STIGLIANO A.A., *La tutela penale del patrimonio informativo aziendale tra appropriazione indebita di files e "presa di conoscenza" di informazioni*, in *Dir. di Internet*, 2020, n. 3, p. 489 ss.
[234] Così anche BARILE L., *Appropriazione indebita di file informatici: tra interpretazione estensiva e divieto di analogia il diritto penale è 'cosa mobile'*, in *Sist. pen.*, 2021, n. 3, p. 139 ss., p. 148 e PICOTTI L., *Studi di diritto penale dell'informatica*, cit., 112, per il quale i dati informatici non sono suscettibili di possesso esclusivo proprio perché possono essere oggetto di autonomo trattamento e godimento senza che altri ne debba perdere la disponibilità.
[235] Possibilità già implicitamente riconosciuta da Cass. pen., sez. V, 23 luglio 2015, n. 32383.
[236] Cass. pen., sez. V, sentenza 13 novembre 2014, n. 47105.

informatica qualora l'apprensione dei dati informatici idonei all'accesso sia finalizzata alla successiva sottrazione del patrimonio dei titolari dei dati. Non solo, ma poiché i nuovi strumenti di pagamento virtuali non sono che un insieme di dati, e ciò vale in particolare per le criptovalute, si pone il problema della configurabilità del "furto" non solo delle credenziali di accesso al sistema informatico, ma anche della stessa moneta elettronica o della valuta virtuale. A tal proposito, si può affermare che il c.d. furto di moneta elettronica si porrebbe in rapporto di incompatibilità con il reato di frode informatica, appositamente introdotto nell'ordinamento proprio per l'impossibilità di ricondurre le nuove modalità di aggressione al patrimonio commesse mediante computer ai reati tradizionali quali truffa e frode informatica. Non appare corretto, dunque, qualificare l'illegittima apprensione di un valore monetario memorizzato elettronicamente come "furto" ex art. 624 c.p., poiché altrimenti si arriverebbe al paradosso di abrogare tacitamente proprio la fattispecie appositamente inserita nel codice penale proprio per sanzionare il trasferimento non consensuale di un valore monetario virtuale, ovvero la frode informatica.

La giurisprudenza in passato ha implicitamente ammesso la configurabilità del concorso tra il c.d. furto di dati, però riferito alla sola copiatura dei dati idonei all'accesso al sistema, e la frode informatica, in caso di loro successivo utilizzo ai fini dell'alterazione del sistema, dunque nel caso di conseguimento del profitto con altrui danno patrimoniale[237]. Tale interpretazione però non tiene conto del fatto che esistono già molteplici norme che sanzionano l'illegittima apprensione dei dati altrui, a partire dall'art. 615-*quater* c.p., norma che sanziona espressamente chi si procura i dati d'accesso all'altrui sistema informatico, condotta, quest'ultima, astrattamente riconducibile anche al c.d. furto o all'appropriazione indebita di dati, qualora questi ultimi siano idonei all'accesso. Qui il momento consumativo è identico, per cui si pone un problema di interferenza tra le due norme. Tale interferenza può riguardare anche il reato di cui all'art. 615-*ter* c.p., qualora il reo effettui previamente un accesso abusivo per procedere alla copiatura dei dati identificativi contenuti nel *server*. A tal proposito, la giurisprudenza di legittimità ha evidenziato che la duplicazione dei dati contenuti in un sistema informatico costituisce condotta tipica del reato di cui all'art. 615-*ter* c.p., dato che l'accesso abusivo può sostanziarsi sia in una semplice lettura dei dati ivi contenuti, sia nella copiatura degli stessi da parte del reo, per cui la condotta di appropriazione indebita di dati si esaurisce in quella del delitto di accesso abusivo e la

[237] In tal senso Cass. pen., sez. V, 23 luglio 2015, n. 32383 cit., che implicitamente ammette la configurabilità del concorso tra le fattispecie di "furto di dati" ex art. 624 c.p. e frode informatica.

violazione dell'art. 646 c.p. deve considerarsi assorbita[238]. Pertanto, per commettere l'appropriazione indebita e, a maggior ragione, il furto di dati, è normativamente imposto un passaggio attraverso la fattispecie di accesso abusivo. Tuttavia, appare corretto ritenere applicabile soltanto la fattispecie di accesso abusivo a sistema informatico o telematico ex art. 615-*ter* c.p., dato che la pretesa di ritenere sussistente il concorso tra tutti i reati elencati (peraltro, si ricorda, sulla base di un'interpretazione piuttosto discutibile del concetto di "cosa mobile") produrrebbe un'ingiustificata moltiplicazione di sanzioni. Tale soluzione può valere anche per quanto riguarda i rapporti tra il furto o l'appropriazione indebita di dati e il diverso reato di cui all'art. 615-*quater* c.p., il quale, peraltro, potrebbe addirittura essere ritenuto speciale per via della specificazione dell'oggetto materiale del reato, ovvero «*codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico*» e non semplice cosa mobile.

In ogni caso, si evidenzia che qualora il "furto" o "l'appropriazione indebita" di dati personali altrui idonei all'accesso ad un sistema informatico o telematico abbia quale scopo la commissione di una frode informatica, tale condotta può essere riconducibile alla fattispecie di frode informatica aggravata dal furto o dall'indebito utilizzo dell'identità digitale, ai sensi dell'art. 640-*ter* co. 3 c.p. fattispecie che può essere considerata reato complesso, comprensiva del disvalore sia dell'illecita apprensione delle credenziali altrui mediante copiatura, sia del loro successivo utilizzo per scopi fraudolenti.

Tale nuovo orientamento in merito alla nozione di "cosa mobile" può avere rilevanza anche con riferimento al fenomeno della compravendita o cessione dei dati altrui illecitamente captati. La giurisprudenza in passato ha escluso che le condotte di furto, danneggiamento, ricettazione e appropriazione indebita potessero aver ad oggetto dei dati in quanto tali, semmai i supporti materiali nei quali gli stessi erano contenuti[239]. In particolare, ha evidenziato che i dati non possono essere ricompresi nel concetto di "cosa", oggetto materiale dei reati citati, in quanto quest'ultimo concetto si riferisce solamente ad oggetti corporei, entità materiali suscettibili di detenzione, sottrazione ed impossessamento, mentre i dati non lo sono, in quanto non è possibile "sottrarre un *file*" o comunque appropriarsene, facendone venir meno con ciò stesso la disponibilità al precedente possessore o titolare. Da ciò deriverebbe l'impossibilità della configurabilità del delitto di ricettazione in caso di

[238] Così Cass. pen., sez. V, 8 luglio 2008, n. 37322.
[239] In tal senso Cass. pen., sez. IV, 29 gennaio 2004, n. 3449; Cass. pen., sez. IV, 21 dicembre 2010, n. 44840; Cass. pen., sez. II, 24 maggio 2016, n. 21596. Per la dottrina v. anche DELL'OSSO A., *Sub art. 648 c.p.*, in *Commentario breve al codice penale*, cit., p. 2312 ss., p. 2313.

compravendita di dati illecitamente captati, in favore dell'applicabilità del diverso reato di cui all'art. 615-*quater* c.p.[240]. Tuttavia, l'interpretazione più recente in merito alla nozione di "cosa mobile" ha dato un'apertura rispetto all'applicabilità del reato di ricettazione alla seconda fase dei *phishing attacks*. Secondo tale tesi, dunque, in caso di compravendita di dati carpiti a seguito di *e-mail* di *phishing* o installazione di *malware* si potrebbe applicare la fattispecie di cui all'art. 648 c.p. Tuttavia, anche in tale caso si può obiettare che tale tesi sovrappone il concetto di "dato informatico" a quello diverso di "cosa mobile", senza tener conto che in realtà non è possibile appropriarsi di un dato informatico facendone venir meno con ciò stesso la disponibilità al precedente possessore o titolare, e in tal modo travalica il divieto di analogia *in malam partem* in materia penale[241].

In ogni caso, anche a seguire tale tesi, il problema della copertura normativa rispetto alle condotte di cui alla seconda fase dei *phishing attacks* non sarebbe definitivamente risolto, in quanto, come noto, il delitto di ricettazione non si applica all'autore del reato presupposto[242] e a coloro che con lui hanno concorso: dunque, se colui che sottrae le *password* altrui è lo stesso che poi le mette in vendita sul *dark web* la norma applicabile resterebbe sempre e solo l'art. 615-*quater* c.p.

11. La difficile individuazione dei rapporti tra le norme incriminatrici

Dall'analisi effettuata emerge l'oggettiva difficoltà per gli interpreti nel riscostruire i rapporti tra i diversi reati sopra esaminati e dunque stabilire quando vi sia concorso effettivo di reati e quando, invece, vi sia concorso apparente di norme. Tale ostacolo ha importanti riflessi sul piano applicativo, poiché l'utilizzo del solo criterio della specialità unilaterale, l'unico ammissibile secondo la giurisprudenza delle Sezioni Unite per verificare se vi sia o meno concorso effettivo di reati comporta il rischio di una moltiplicazione delle contestazioni per fatti che in realtà si pongono tra loro in rapporto di stretta interdipendenza, quali ad esempio l'accesso abusivo commesso al fine di realizzare una frode informatica o un danneggiamento informatico. Con riferimento alle fattispecie descritte, quindi, l'esigenza di vagliare la possibilità di applicare criteri differenti per tracciare il confine tra concorso di

[240] Cass. pen., sez. II, sentenza 3 ottobre 2013, n. 47021.
[241] In tal senso v. BARILE L., *Appropriazione indebita di file informatici*, cit., p. 148 e PICOTTI L., *Studi di diritto penale dell'informatica*, cit., 112, per il quale i dati informatici non sono suscettibili di possesso esclusivo proprio perché possono essere oggetto di autonomo trattamento e godimento senza che altri ne debba perdere la disponibilità.
[242] DELL'OSSO A., *Sub art. 648 c.p.*, cit., p. 2313.

reati e concorso apparente di norme è particolarmente sentita, anche per un'esigenza di rispetto del principio fondamentale di proporzione tra fatto illecito e pena.

È pur vero che a mitigare il trattamento sanzionatorio vi è comunque l'art. 81 c.p., in particolare il co. 2[243], e che tra le fattispecie sopra descritte, anche qualora si ritenesse che il concorso sia materiale, si potrebbe ravvisare comunque la sussistenza del medesimo disegno criminoso[244]. La presenza di tale ultima norma, però, di per sé non è risolutiva, perché i rapporti tra le diverse fattispecie sono tutt'altro che ben definiti, basti pensare alle pronunce giurisprudenziali discordanti in merito ai rapporti tra accesso abusivo a sistema informatico o telematico e detenzione e diffusione abusiva di codici di accesso. Resta, dunque, il problema dell'ingiustificata disparità di trattamento, poiché, in assenza di un criterio univoco, il numero di fattispecie di volta in volta contestabile in relazione agli stessi identici fenomeni criminosi rimane indefinito. Tale discrezionalità nella scelta del numero di fattispecie applicabile si traduce nella violazione del principio di uguaglianza, dato che lo stesso comportamento, come ad esempio l'installazione di un programma volto a formattare un dispositivo informatico altrui, può, a seconda dei casi e dei reati che il singolo magistrato inquirente abbia deciso di contestare, essere punito, ad esempio, come mero danneggiamento informatico, o accesso abusivo a sistema informatico aggravato dalla violenza sulle cose oppure come danneggiamento informatico e accesso abusivo in concorso tra loro.

La possibilità di utilizzare il diverso criterio della consunzione/assorbimento potrebbe essere una soluzione idonea ad evitare queste disparità di trattamento e restituirebbe coerenza al sistema normativo. A tal proposito, si evidenzia che tale criterio non fa leva sul mero atteggiarsi del fatto concreto, ma richiede comunque un confronto strutturale tra le norme, poiché occorre verificare se la condotta meno grave risulti secondo l'*id quod plerumque accidit*, una conseguenza normale e prevedibile del più grave reato assorbente e, dunque, valutare se il legislatore abbia già tenuto in considerazione anche gli ulteriori ordinari sviluppi della condotta incriminata dal reato più grave. Inoltre, occorre verificare che la violazione più grave tuteli, non necessariamente in via esclusiva, anche beni giuridici

[243] Si evidenzia, infatti, che se le condotte sono realizzate l'una successivamente all'altra, come nel caso, ad esempio, degli artt. 615-*ter* e 615-*quater* c.p., esse danno vita ad una pluralità di azioni e, dunque, ad un concorso materiale di reati. Sul punto v. ZAGREBELSKY V., *Reato continuato*, Milano, 1976, p. 101 ss.; DE FRANCESCO G., *Lex specialis*, cit., p. 68.

[244] Proprio la presenza di tale norma ha indotto Cass. pen., sez. un., 23 febbraio 2017, n. 20664 cit. a escludere che l'utilizzo del solo principio di specialità si ponga in contrasto con le esigenze di giustizia sostanziale di correlazione della sanzione alla gravità del fatto. Sulla nozione di medesimo disegno criminoso v. AMBROSETTI E.M., *Problemi attuali in tema di reato continuato. Dalla novella del 1974 al nuovo codice di procedura penale*, Padova, 1991, p. 22 ss.

omogenei rispetto a quelli tutelati dal reato meno grave[245]. Peraltro, nel diritto penale dell'informatica, il parametro del bene giuridico tutelato svolge un ruolo particolarmente importante, perché permette di valorizzare le connessioni, gli elementi comuni e quelli differenziali delle singole fattispecie, in un insieme di norme che, come si è potuto constatare, sono frammentarie e scarsamente coordinate tra di loro[246]. Il criterio dell'assorbimento, dunque, che valorizza proprio tale rilevante profilo, potrebbe anche restituire unitarietà e coerenza a questo settore del diritto penale.

Tuttavia, vi è un grosso ostacolo all'applicazione *tout court* di tale principio in questo settore, ovvero il trattamento sanzionatorio delle diverse fattispecie: l'art. 617-*quater* e l'art. 617-*quinquies* c.p., ad esempio, sono puniti con pena molto superiore rispetto a quella prevista dall'art. 615-*ter* c.p. sull'accesso abusivo, per cui difficilmente si può ritenere tali due reati assorbibili in quest'ultimo. Né tra le fattispecie esaminate si riesce ad individuare un reato complesso che, ai sensi dell'art. 84 c.p. ricomprenda al suo interno tutti gli elementi costitutivi delle altre fattispecie e assorba il disvalore complessivo del fatto[247].

Inoltre, qualora il criterio dell'assorbimento fosse applicabile in ragione del trattamento sanzionatorio, basti pensare agli artt. 615-*quater* e 615-*ter* c.p., rimane il problema del diverso regime di procedibilità. Pertanto, sarebbe da superare il principio per cui l'assorbimento non attiene al rapporto astratto tra le fattispecie, ma solo alla dimensione concreta del fatto, perché tale assunto comporta conseguenze paradossali, come ad esempio nei casi di remissione di querela per i reati di accesso abusivo a sistema informatico o telematico o di danneggiamento informatico[248]. Infatti, se si considera la consunzione dell'antefatto esclusivamente come vicenda che attiene alla dimensione concreta della pena da irrogare, qualora il reato più grave non sia punibile, l'imputato dovrebbe comunque rispondere del reato meno grave, quali ad esempio i reati di cui agli artt. 615-*quater* e 615-*quinquies* c.p., nonostante la vittima, con la rimessione di querela, abbia manifestato la sua volontà che il reato più grave commesso a suo danno non sia più punito. È evidente l'irragionevolezza di tale disciplina, a maggior ragione se si considera che, invece, quando

[245] FINOCCHIARO S., *Il buio oltre la specialità. Le Sezioni Unite sul concorso tra truffa aggravata e malversazione*, in *Dir. pen. cont.*, 2017, n. 5, p. 344 ss., p. 348.
[246] Così anche PICOTTI L., *Sistematica*, cit., p. 22 s.
[247] Reato complesso che, per alcuni, può essere ricondotto al principio di assorbimento, così PAGLIARO A., voce *Concorso di norme*, cit., p. 552; PROSDOCIMI S., *Reato complesso*, in *Dig. pen.*, vol. XI, Torino, 1996, p. 213 ss., p. 216 ss. *Contra* FROSALI R.A., *Concorso di norme e concorso di reati*, Milano, 1971, p. 410, che ritiene che il reato complesso rientri più propriamente in un generale caso di specialità ex art. 15 c.p. piuttosto che in una relazione di assorbimento.
[248] La stessa Cass. pen. 21987/2019 cit. sostiene che l'assorbimento del delitto meno grave di cui all'art. 615-*quater* c.p. nel più grave di cui all'art. 615-*ter* c.p. può operare solo se quest'ultimo sia contestato e procedibile.

le norme sono tra loro in rapporto di specialità, qualora il reato speciale non sia punibile non si ha reviviscenza della norma generale[249].

Il sistema complessivo dei reati contro la riservatezza informatica e a tutela delle comunicazioni informatiche e telematiche, dunque, necessita quanto prima di un riordino da parte del legislatore, che dovrebbe eliminare tutte le duplicazioni esistenti, magari "accorpando" le norme di cui agli artt. 617-*quater*, 617-*quinquies* e 617-*sexies* c.p. con le corrispondenti fattispecie a tutela della riservatezza delle comunicazioni, introducendo una clausola generale di estensione, in modo da evitare l'interferenza tra le diverse fattispecie.

12. Considerazioni di sintesi

Il sistema dei reati contro la riservatezza informatica e a tutela delle comunicazioni informatiche e telematiche è composto da una moltitudine di fattispecie, che si trovano quasi sempre in rapporto di interferenza tra di loro e, come si esaminerà nel prossimo capitolo, che concorrono con i reati specificamente posti a tutela del patrimonio. In tale ambito il legislatore ha fatto un uso sin troppo parsimonioso delle clausole di sussidiarietà espressa, le quali, invece, avrebbero contribuito a razionalizzare una materia che è diventata davvero caotica, dato il numero abnorme di fattispecie applicabili a fenomeni quali il *phishing* o lo *skimming*.

Risulta però evidente che in questo sistema assolutamente sovrabbondante e ricco di fattispecie spesso tra loro del tutto simili e la cui distinzione in alcuni casi è basata unicamente sul fine criminoso, rimane sostanzialmente priva di sanzione penale la c.d. seconda fase dei *phishing attacks*, la più delicata poiché concerne la vendita di *virus* e credenziali altrui, nonché in generale il fenomeno del *Cybercrime-as-a-service*. A meno di qualificare i dati informatici come "cosa mobile" e ritenere applicabile la fattispecie di ricettazione, con tutti i problemi conseguenti sopra evidenziati, la tutela di tale fase, infatti, resta sostanzialmente affidata agli artt. 615-*quater* e 615-*quinquies* c.p., i quali, però, come sopra evidenziato, sono norme a più fattispecie e con pene piuttosto basse e non idonee con riferimento a fenomeni complessi quale il *Cybercrime-as-a-service*. Escluso, dunque, il caso in cui venga accertata l'esistenza di un'associazione a delinquere dedita alla vendita di *malware*, i soggetti dediti alla vendita delle credenziali di autenticazione bancarie, *password*, numeri di carte di credito, ecc. anche in modo sistematico e professionale vengono sanzionati

[249] Così MANTOVANI F., *Concorso e conflitto di norme nel diritto penale*, Bologna, 1966, p. 697 ss. e FROSALI R.A., *Concorso di norme e concorso di reati*, cit., p. 370, che evidenziano che la deroga di cui all'art. 15 incide sulla validità della norma generale.

con pene piuttosto lievi, al pari degli acquirenti o dei "possessori" di tali oggetti. Pertanto, più che il possesso sarebbe meglio sanzionare la compravendita di programmi, dati, *password*, numeri di carte di credito, ecc., magari differenziando la responsabilità penale e prevedendo pene più elevate per i soggetti dediti alla vendita di tali oggetti in modo sistematico. Più che all'oggettiva finalità del programma e fine dell'agente bisognerebbe dare rilevanza centrale proprio alla condotta, in modo tale che anche in queste fattispecie sia quest'ultima ad avere un ruolo centrale.

Dunque, nonostante il numero davvero elevato di fattispecie volte a sanzionare la prima fase degli attacchi informatici contro il patrimonio, non esistono fattispecie realmente adeguate a sanzionare anche la successiva fase della messa a disposizione o "compravendita" di *malware, ransomware*, ecc. Infatti, alla seconda fase trovano applicazione le fattispecie previste specificamente per la prima fase, le quali presentano tutte un numero davvero elevato di condotte sanzionate, peraltro quasi identiche tra loro (con pochissime eccezioni), dando così origine ad un problema di interferenza tra fattispecie.

Si evidenzia che il problema sopra esaminato non è relativo unicamente alle fattispecie esaminate in questo capitolo. Infatti, i reati esaminati in questo capitolo sanzionano solo le prime fasi degli attacchi informatici contro il patrimonio, ma la fase dell'effettivo depauperamento della vittima comporta l'applicazione anche delle ulteriori fattispecie poste specificamente a tutela del patrimonio. Dunque, nel prossimo capitolo si esamineranno proprio queste ultime fattispecie nonché quelle in generale poste a tutela dei mezzi di pagamento e i loro rapporti con i reati esaminati in questo capitolo.

Capitolo III

I reati *latu sensu* patrimoniali nell'ordinamento italiano: problemi applicativi

Sommario: 1. I tradizionali reati di truffa ed estorsione alla prova delle nuove minacce cibernetiche al patrimonio; 1.1. Il reato di truffa; 1.2. Le truffe *online* e la circostanza aggravante della minorata difesa; 1.3. L'individuazione del *locus commissi delicti*; 1.4. L'estorsione. - 2. La frode informatica ex art. 640-*ter* c.p. e i suoi ambiti applicativi. - 2.1 L'ipotesi aggravata dal «furto o indebito utilizzo dell'identità digitale». -2.2 La nuova circostanza aggravante del fatto che «produce un trasferimento di denaro, di valore monetario o di valuta virtuale». - 3. Il reato di indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti ex art. 493-*ter* c.p. - 4. Il microsistema normativo dei danneggiamenti informatici. - 5. Concorso di reati. – 6. Il concorso di persone nel reato - 7. Considerazioni di sintesi.

1. I tradizionali reati di truffa ed estorsione alla prova delle nuove minacce cibernetiche al patrimonio

Alcune delle diverse minacce cui è esposto il patrimonio nel *web* non sono che evoluzioni di tradizionali schemi di truffe, che venivano e vengono tutt'ora perpetrate nel mondo reale. A ben guardare, però, anche alcune moderne manifestazioni criminose contro il patrimonio apparse negli ultimi anni, ad esempio l'impiego dei *ransomware*, anche se agiscono direttamente sui sistemi informatici in realtà costituiscono una nuova modalità di commissione di tradizionali fattispecie contro il patrimonio.

Si può, dunque, affermare che oggi le moderne tecnologie informatiche consentono di commettere molteplici schemi di truffe e di estorsioni nel *web*. Tuttavia, la commissione del fatto criminoso *online* o la direzione dell'azione contro lo strumento informatico non sono elementi neutri e possono dare adito a diversi problemi applicativi. Vanno, pertanto, prima esaminate le difficoltà che potrebbero insorgere e poi, su tale base, va stabilito se le tradizionali fattispecie di truffa ed estorsione siano realmente idonee a sanzionare le nuove minacce cibernetiche dirette contro il patrimonio.

1.1 Il reato di truffa

La prima fattispecie che viene in evidenza è quella della truffa, di cui all'art. 640 c.p., che sanziona chiunque, mediante artifici e raggiri, inducendo taluno in errore, procura a sé

o ad altri un ingiusto profitto con altrui danno. Il bene giuridico tutelato dalla norma in questione è sicuramente il patrimonio, ma in dottrina si è discusso a lungo sull'ipotetica natura plurioffensiva della truffa. In particolare, vi è chi ritiene che la truffa tuteli anche la libertà di autodeterminazione[1].

La truffa può essere commessa da chiunque nei confronti di chiunque, per cui si tratta di un reato comune[2]. Il destinatario degli artifici o raggiri, però, può essere solo una persona fisica, in quanto tale oppure quale titolare di un organo pubblico o privato[3]. È poi necessario che il soggetto passivo sia capace di intendere e di volere, altrimenti il fatto integra altre fattispecie quali il furto o la circonvenzione di incapaci[4].

Trattasi di reato a condotta vincolata, perché la condotta di aggressione al patrimonio è penalmente rilevante solo se viene perpetrata attraverso artifizi o raggiri[5]. Non sono mancate però opinioni differenti, secondo cui in realtà la truffa sarebbe reato a forma libera, che può essere cagionata da ogni mezzo che abbia indotto in errore ed abbia sorpreso la buona fede del soggetto passivo[6]. Si evidenzia, però, che tale tesi è palesemente contraria al principio di tipicità e frammentarietà del diritto penale, perché l'utilizzo da parte del legislatore della formula "artifici e raggiri" è indice del fatto che non abbia voluto sanzionare tutte le condotte fraudolente aggressive del patrimonio[7]. Ciò, però, non significa che sia necessaria una particolare attitudine o idoneità ingannatoria del mezzo usato, che, invece, era richiesta nel precedente codice Zanardelli.

Per "artifizio" si intende qualsiasi trasfigurazione del vero, ossia qualsiasi camuffamento della realtà effettuato sia simulando ciò che non esiste, sia dissimulando ciò che esiste, mentre per "raggiro" si intende un artificio dialettico o insieme di parole

---

[1] ANGELOTTI D., *op. cit.*, p. 393; DE MARSICO A., *Delitti contro il patrimonio*, cit., p. 2 ss.; ANTOLISEI F., *Manuale di diritto penale. PS*, cit., p. 472. Critico invece ZANNOTTI R., *La truffa*, Milano, 1993, p. 14, il quale ritiene che quando si afferma che l'interesse protetto dalla norma debba ravvisarsi anche nella tutela e libertà del consenso o della buona fede, si confonde l'interesse protetto col mezzo che il legislatore richiede per arrecare l'offesa patrimoniale. Nello stesso senso anche MARINI G., *voce Truffa (diritto penale)*, in *Noviss. Dig. It.*, vol. XIX, Torino, 1973, p. 864 ss., p. 866.

[2] MAGGINI A., *La truffa*, Padova, 1988, p. 3; MARINI G., *voce Truffa*, cit., p. 868.

[3] MARINI G., *voce Truffa*, cit., p. 869; ZANNOTTI R., *La truffa*, cit., p. 54.

[4] PEDRAZZI C., *Inganno ed errore*, cit., p. 111; ANGELOTTI D., *op. cit.*, p. 400. Sottolinea ROTOLO G., *Sub art. 640 c.p.*, in *Commentario breve al codice penale*, cit., p. 2258, p. 2260, che sul punto in dottrina e giurisprudenza si registra comunanza di vedute.

[5] LUCARELLI U., *La truffa. Aspetti penali, civili e processuali*, Padova, 2002, p. 10; ZANNOTTI R., *La truffa*, cit., p. 21.

[6] Così ANGELOTTI D., *op. cit.*, p. 406, secondo cui «*la rassegna dei vari mezzi che possono realizzare un ingiusto profitto con altrui danno, dimostra come sia del tutto insufficiente la formula "mediante artifizi o raggiri" a contenere tutti i mezzi di consumazione di tale delitto*».

[7] SAMMARCO G., *La truffa contrattuale*, Milano, 1988, p. 66; ZANNOTTI R., *La truffa*, cit., p. 21; LUCARELLI U., *La truffa*, cit., p. 11.

congegnate e finalizzate a trarre in inganno la vittima[8]. La differenza tra i due è che l'artifizio opera sulla realtà esterna, creando una falsa apparenza materiale, mentre il raggiro agisce direttamente sulla psiche dell'ingannato[9]. Essi possono indifferentemente coesistere o ricorrere singolarmente[10], ma è necessario che precedano sempre l'induzione in errore e il conseguimento dell'ingiusto profitto[11].

Si è posto il problema se la mera menzogna possa costituire un artificio o un raggiro. Per molti autori essa, pur potendo essere costitutiva di uno schema fraudolento, ai fini della rilevanza penale necessita comunque di un *quid pluris* costituito dalle note modali caratterizzanti gli "*artifici e raggiri*"[12]. La giurisprudenza prevalente, invece, ha finito per ammettere che anche la semplice menzogna possa bastare per dar vita alla truffa[13]. Tale divergenza si verifica anche con riferimento alla configurabilità della truffa in forma omissiva. Infatti, la dottrina prevalente nega tale possibilità, evidenziando che la qualificazione della truffa quale reato a forma vincolata comporta per forza di cose l'incompatibilità della truffa con una realizzazione in forma omissiva[14]. Al contrario, la giurisprudenza prevalente la ammette, limitandosi a richiedere la verifica della avvenuta violazione da parte del soggetto attivo di un obbligo giuridico di rivelare le circostanze taciute e stimando *tout court* tale comportamento di per sé idoneo a trarre dolosamente in errore, perché preordinato a perpetrare l'inganno. In particolare, si ritiene che la fonte dell'obbligo giuridico violato possa risiedere anche in norme extrapenali quali gli artt. 1377 o 1759 c.c.[15].

Il comportamento dell'agente deve determinare un errore, ovvero deve essere causa di un inganno. Per induzione in errore, infatti, si intende l'incidenza sull'altrui volontà,

---

[8] ANTOLISEI F., *Manuale di diritto penale. PS*, cit., p. 474.
[9] *Ibid*., p. 475.
[10] LUCARELLI U., *La truffa*, cit., p. 10.
[11] Cass. pen., sez. II pen., sentenza 15 febbraio 2017, n. 9197.
[12] SAMMARCO G., *La truffa contrattuale*, cit., p. 190; LUCARELLI U., *La truffa*, cit., p. 19. MANTOVANI F., *Contributo allo studio della condotta*, cit., p. 211. Al contrario, per MARINI G., *voce Truffa*, cit., p. 873 la condotta può certamente consistere nel mero mendacio, posto che «*la condotta di truffa consiste, sostanzialmente, in un mendacio*».
[13] In tal senso Cass Sez. 3, n. 3046 del 10/11/1965 Rv. 100665; Cass. Sez. 2 n. 2061 del 19/10/1971; Cass. sez. 5 n. 8558 del 21/05/1979; Cass. Sez. 6, n. 8787 del 19/06/1981; Cass. Sez. 2, n. 9426 del 05/02/1982; Cass. Sez. 2, n. 10206 del 14/5/1982. Più di recente anche Cass. pen., sez. feriale, sentenza 2 settembre 2010, n. 42719; Cass. pen., sez. II, 7 aprile 2006, n. 17513.
[14] MAGGINI A., *La truffa*, cit., p. 15; ZANNOTTI R., *La truffa*, cit., p. 31; PEDRAZZI C., *Inganno ed errore*, cit., p. 218 attribuisce rilevanza al silenzio solo nel caso in cui esso costituisca violazione degli obblighi di buona fede e sia interpretato dal soggetto passivo come una condotta concludente ed in tale veste abbia provocato l'induzione in errore.
[15] Cass. pen., sez. II, sentenza 14 ottobre 2009, n. 41717; Cass. pen., sez. II, sentenza 21 giugno 2005, n. 33466; Cass. pen., sez. II, sentenza 13 novembre 1997, n. 870.

operando mediante la persuasione o altre modalità[16]. Non si richiede più, come nel codice Zanardelli, il requisito dell'attitudine del mezzo ad ingannare o sorprendere, ma è sufficiente che in concreto il mezzo utilizzato abbia cagionato l'inganno[17].

L'errore del soggetto passivo è requisito fondamentale della truffa, tanto che da alcuni autori viene qualificato come l'evento intermedio della fattispecie[18]. Esso va inteso come contenuto psichico positivo, ovvero come presenza attuale di un convincimento non conforme a verità[19] e può essere di fatto o di diritto[20]. Esso si distingue dall'ignoranza perché quest'ultima rimane nella sfera psichica del soggetto agente e può generare un errore solo nel momento in cui un soggetto trasforma il suo pensiero in comportamento[21].

La teoria vittimo-dogmatica, a differenza che in altri ordinamenti, non ha trovato accoglimento nell'ordinamento giuridico italiano. Si è evidenziato, infatti, che se per l'effettiva configurabilità della fattispecie dovesse essere esaminata la presenza di un requisito non scritto, ovvero l'avvenuta attivazione o l'impossibilità di attivazione da parte della vittima di misure a difesa del bene giuridico, la norma non risulterebbe sufficientemente determinata, poiché i contorni di tale requisito non appaiono individuabili con sicurezza[22]. Inoltre, si ritiene che l'interpretazione vittimologica si ponga in contrasto con principi irrinunciabili di rango costituzionale, quali il supremo principio solidaristico, secondo cui è lo Stato ad essere istituzionalmente preposto a difendere in via principale i beni dei consociati, mentre questi ultimi possono (non devono) difendersi solo qualora lo Stato non sia presente[23]. Per cui non può affatto escludersi la tipicità del reato di truffa in caso di negligenza della vittima, caduta in errore in presenza di circostanze tali che avrebbero potuto impedire l'evento ingannatorio[24]. Anche la giurisprudenza ha precisato che la mancanza di diligenza da parte della vittima non rileva ai fini dell'integrazione del reato in esame[25].

---

[16] ROTOLO G., *Sub art. 640 c.p.*, cit., p. 2266.
[17] ANTOLISEI F., *Manuale di diritto penale. PS*, cit., p. 477.
[18] MAGGINI A., *La truffa*, cit., p. 23.
[19] PEDRAZZI C., *Inganno ed errore*, cit., p. 125.
[20] MARINI G., *voce Truffa*, cit., p. 881.
[21] LUCARELLI U., *La truffa*, cit., p. 27.
[22] DEL TUFO V., *Profili critici della vittimo-dommatica. Comportamento della vittima e delitto di truffa*, Napoli, 1990, p. 266 s.
[23] DEL TUFO V., *Profili critici della vittimo-dommatica*, cit., p. 247 s.; LUCARELLI U., *La truffa*, cit., p. 35.
[24] LUCARELLI U., *La truffa*, cit., p. 36.
[25] V. Cass. pen., sez. II, sentenza 20 novembre 2019, n. 51538, secondo cui «*ai fini della sussistenza del delitto di truffa, non ha rilievo la mancanza di diligenza da parte della persona offesa, dal momento che tale circostanza non esclude l'idoneità del mezzo, risolvendosi in una mera deficienza di attenzione spesso determinata dalla fiducia ottenuta con artifici e raggiri*»; In senso conforme anche Cass. pen., sez. II, sentenza 20 giugno 2017, n. 42867; Cass. pen., sez. II, sentenza 25 settembre 2014, n. 42941; Cass. pen., sez. II, sentenza 17 marzo 1993, n. 4011.

Si è posto il problema dell'ipotesi della c.d. truffa a tre soggetti, ovvero di quei casi in cui il soggetto raggirato ed indotto in errore è diverso da quello nei cui confronti si trae l'ingiusto profitto. Oggi si ammette la configurabilità della truffa anche nei casi in cui l'autore dell'atto dispositivo e il titolare del patrimonio aggredito non siano la stessa persona, come avviene nei casi dei soggetti abilitati ad agire sul patrimonio altrui[26]. A tal proposito, infatti, si sottolinea che dalla formulazione della norma non si ricava alcuna preclusione al riguardo. Si evidenzia, però, che non può integrare gli estremi della truffa ogni atto frutto di una condotta fraudolenta altrui da cui derivino effetti pregiudizievoli nella sfera giuridico-patrimoniale di un terzo, ma solo quello che si collochi in una prospettiva dispositiva e di omogeneità con l'atto che avrebbe potuto porre in essere il titolare del patrimonio aggredito[27]. Inoltre, è necessario che gli effetti dell'inganno e della condotta dell'ingannato si riverberino sul patrimonio del danneggiato, per cui la persona ingannata deve avere il potere di incidere sul patrimonio del soggetto danneggiato[28].

Nella struttura della truffa viene individuato il requisito implicito dell'atto di disposizione patrimoniale[29]. Si evidenzia infatti che l'errore, essendo elemento puramente conoscitivo, non può essere di per sé stesso causa del danno patrimoniale. Anche in questo caso è necessaria la sussistenza di un nesso di interdipendenza tra l'errore e l'atto di disposizione[30]. L'atto di disposizione patrimoniale viene inteso come qualsiasi comportamento della vittima, dotato di una propria efficacia di fatto, al quale possa ricollegarsi un danno con profitto ingiusto altrui[31]. Esso può essere soltanto quello voluto, sia per quanto riguarda l'oggetto materiale, sia per quanto riguarda i poteri ad altri trasmessi sulla cosa[32]. Nell'ipotesi in cui l'atto di disposizione assuma la forma del contratto, la truffa viene denominata truffa contrattuale, che si verifica quando gli artifizi e raggiri intervengono

[26] PEDRAZZI C., *Inganno ed errore*, cit., p. 97 e 99; MAGGINI A., *La truffa*, cit., p. 3; ZANNOTTI R., *La truffa*, cit., p. 55. In giurisprudenza v. Cass. pen., sez. II, sentenza 21 ottobre 2021, n. 43119; Cass. pen., sez. II, sentenza 19 novembre 2019, n. 46865; Cass. pen., sez. II, sentenza 5 settembre 2018, n. 39958; Cass. pen., sez. II, sentenza 20 gennaio 2016, n. 2281; Cass. pen., sez. II, 17 luglio 2013, n. 43143. *Contra* però Cass. pen., sez. VI, sentenza 22 settembre 2020, n. 28957.
[27] LUCARELLI U., *La truffa*, cit., p. 60.
[28] MAGGINI A., *La truffa*, cit., p. 3.
[29] ZANNOTTI R., *La truffa*, cit., p. 62; MARINI G., *voce Truffa*, cit., p. 881; PEDRAZZI C., *Inganno ed errore*, cit., p. 61 ss.; MANTOVANI F., *Contributo allo studio della condotta*, cit., p. 179. *Contra* PECORELLA G., *voce Patrimonio*, cit., p. 643, il quale, pur ritenendo che il modello più comune di truffa sia caratterizzato da un atto di disposizione della vittima, nega che lo stesso faccia parte della struttura tipica del reato, escludendo che esso possa essere considerato elemento necessario dello stesso.
[30] SAMMARCO G., *La truffa contrattuale*, cit., p. 147.
[31] ZANNOTTI R., *La truffa*, cit., p. 85.
[32] MANTOVANI F., *Contributo allo studio della condotta*, cit., p. 198; PEDRAZZI C., *Inganno ed errore*, cit., p. 126.

nella fase di formazione del negozio ed inducono il soggetto passivo a prestare il consenso, che altrimenti non avrebbe prestato[33].

Come sopra accennato, la truffa è un reato di evento. In particolare, costituiscono eventi del reato di truffa il profitto e il danno[34]. Mentre in molti altri reati contro il patrimonio il profitto è l'oggetto del fine tipico perseguito dall'agente, che però non è necessario sia conseguito ai fini della consumazione, nella truffa il profitto costituisce un vero e proprio elemento costitutivo del reato, la cui verificazione costituisce il momento consumativo dell'illecito[35]. Dunque, la truffa sussiste solo se la condizione patrimoniale generale della vittima rivela a seguito della disposizione un *minus* rispetto alla condizione precedente[36]. A tal proposito, si evidenzia che la mera stipulazione di un contratto in quanto tale non porta a nessuna effettiva diminuzione patrimoniale, perché per la consumazione del reato in questione serve l'alterazione dell'equilibrio giuridico o mutamento in peggio[37].

Per quanto riguarda la nozione di ingiusto profitto, essa può comprendere in sé qualsiasi utilità, incremento o vantaggio, anche a carattere non strettamente economico[38]. Con riferimento al requisito dell'ingiustizia, dottrina e giurisprudenza maggioritarie ritengono che tale requisito consista nella mera mancanza di una giusta causa o di un titolo di legittimazione dell'accrescimento patrimoniale conseguito[39]. Il danno, invece, deve necessariamente avere contenuto patrimoniale[40].

Il danno viene comunemente inteso secondo due differenti accezioni, che muovono dalla differente concezione del patrimonio. Un primo gruppo di autori, che muove dalla concezione giuridica di patrimonio, ritiene che il danno debba essere ritenuto esistente nel momento in cui il patrimonio, inteso come complesso di rapporti giuridico-patrimoniali,

---

[33] SAMMARCO G., *La truffa contrattuale*, cit., p. 11.
[34] MAGGINI A., *La truffa*, cit., p. 25.
[35] ROTOLO G., *Sub art. 640 c.p.*, cit., p. 2269.
[36] SAMMARCO G., *La truffa contrattuale*, cit., p. 40.
[37] BETTIOL G., *Concetto penalistico di patrimonio e momento consumativo della truffa*, in *Giur. it.*, 1947, parte IV, oggi anche in Id., *Scritti giuridici*, vol. II, Padova, 1966, p. 713 ss., p. 716, secondo cui «*il concetto di danno e il concetto di profitto che sono momenti decisivi a proposito della truffa non possono venire evaporati in una considerazione puramente formale per la quale essi debbono considerarsi come già presenti ed operanti nel momento della costituzione di un rapporto obbligatorio (sia pure viziato) e non nel momento in cui tale rapporto produce i suoi effetti concreti. Tra possibilità di un danno e di un profitto ed effettività degli stessi sussiste oltre che una differenza logica anche una differenza reale*». Negli stessi termini anche SAMMARCO G., *La truffa contrattuale*, cit., p. 36.
[38] ANTOLISEI F., *Manuale di diritto penale. PS*, cit., p. 482. In giurisprudenza v. Cass. pen., sez. II, 24 ottobre 2003, n. 42790; Cass. pen., sez. II, sentenza 17 giugno 2003, n. 28894; Cass. pen., sez. VI, sentenza 8 maggio 1998, n. 8443. Contrario a negare la natura patrimoniale del profitto è MARINI G., *voce Truffa*, cit., p. 885.
[39] ROTOLO G., *Sub art. 640 c.p.*, cit., p. 2269.
[40] RAGNO G., *Contributo alla configurazione del delitto di truffa processuale*, Milano, 1966, p. 130, il quale evidenzia che colui che è indotto in errore deve necessariamente adottare una decisione che danneggia il suo patrimonio o quello altrui.

perde una situazione favorevole o acquista una situazione sfavorevole: dunque indipendentemente dall'effettivo verificarsi di una *deminutio patrimonii* dovuta all'esecuzione degli impegni assunti[41]. Diversamente, la dottrina maggioritaria ritiene vi sia un danno in tutti quei casi in cui la vittima si trovi a dover sopportare una diminuzione del proprio patrimonio, intesa come danno emergente o lucro cessante[42]. Anche nella giurisprudenza della Cassazione vi sono state divergenze, tant'è che sul punto si sono ripetutamente pronunciate le Sezioni Unite, le quali hanno dapprima stabilito che il reato di truffa si consuma con l'effettivo conseguimento da parte dell'agente di un bene economico o di altro bene suscettibile di valutazione patrimoniale e con la definitiva perdita dello stesso da parte del soggetto passivo[43], e successivamente hanno ribadito che il danno rilevante ai fini dell'art. 640 c.p. è esclusivamente il danno avente necessariamente un contenuto economico, che dev'essere altresì effettivo e non meramente potenziale[44]. La concezione economica del danno patrimoniale, dunque, è oggi accolta dalla giurisprudenza dominante[45].

Per quanto riguarda l'elemento soggettivo, esso è costituito dal dolo generico: perché si abbia consumazione della truffa è necessario che tutti gli elementi oggetto del dolo si verifichino concretamente, mentre la loro rappresentazione non deve necessariamente costituire motivo della condotta del reo[46]. Inoltre, il dolo non dev'essere limitato al dolo intenzionale, ma può essere anche diretto ed eventuale[47]. In giurisprudenza si è poi affermata la necessità che il dolo copra anche la patrimonialità del danno; dunque, il soggetto deve prevedere e voler realizzare con la propria condotta un danno a contenuto patrimoniale[48].

Al co. 2 dell'art. 640 c.p. sono poi previste una serie di circostanze aggravanti ad effetto speciale, di natura oggettiva[49]. In particolare, al n. 1 si fa riferimento al fatto commesso a danno dello Stato o di altro ente pubblico o dell'Unione europea o col pretesto di far esonerare taluno dal servizio militare. Al n. 2 del co. 2 art. 640 c.p. è poi presente la circostanza aggravante del fatto commesso ingenerando nella persona offesa il timore di un

---

[41] DELOGU T., *Il momento consumativo della truffa*, in *Giur. Cass. pen.*, 1944, vol. XIV, p. 68 ss., p. 70 ss.; DE MARSICO A., *Delitti contro il patrimonio*, cit., p. 146.
[42] PEDRAZZI C., *Inganno ed errore*, cit., p. 20 ss.; SGUBBI F., *voce Patrimonio (reati contro il)*, cit., p. 378; ZANNOTTI R., *La truffa*, cit., p. 93; MAGGINI A., *La truffa*, cit., p. 25.
[43] Cass. pen., Sez. Un., sentenza 22 marzo 1969, in Foro It., 1970, Vol. 93, n. 1, p. 5 ss.
[44] Cass. pen., Sez. Un., sentenza 16 dicembre 1998, n. 1 e Cass. pen., Sez. Un., sentenza 1 agosto 2000, n. 18.
[45] In tal senso v. Cass. pen., sez. II, sentenza 14 maggio 2014, n. 34722; Cass. pen., sez. II, sentenza 15 gennaio 2013, n. 18762; Cass. pen., sez. II, sentenza 17 giugno 2011, n. 25956.
[46] MARINI G., *voce Truffa*, cit., p. 886; ZANNOTTI R., *La truffa*, cit., p. 117. È rimasta isolata l'opinione di DE MARSICO A., *Delitti contro il patrimonio*, cit., p. 148, secondo cui la norma in questione richiederebbe il dolo specifico.
[47] LUCARELLI U., *La truffa*, cit., p. 113.
[48] Cass. pen., sez. II, sentenza 17 giugno 2011, n. 25956.
[49] LUCARELLI U., *La truffa*, cit., p. 142.

pericolo immaginario o l'erroneo convincimento di dovere eseguire un ordine dell'Autorità. Infine, al n. 2-*bis* del co. 2, inserito dall'art. 3 co. 28 della l. 15 luglio 2009, n. 94, si fa riferimento alla circostanza aggravante di cui all'art. 61 co. 5 c.p., vale a dire l'aver profittato di circostanze di tempo, di luogo o di persona, anche in riferimento all'età, tali da ostacolare la pubblica o privata difesa. Quest'ultima circostanza aggravante, in particolare, come si esaminerà meglio nel prosieguo, assume speciale rilevanza con riferimento alle condotte poste in essere nel *web*.

1.2. Le truffe *online* e la circostanza aggravante della minorata difesa

Come evidenziato, con lo sviluppo e diffusione del *web* si è assistito all'evoluzione e proliferazione di schemi tradizionali di truffa, quali gli *advance fee fraud schemes* o gli schemi Ponzi. La totalità di essi ben può rientrare nell'ambito applicativo dell'art. 640 c.p. Infatti, il fatto che lo schema fraudolento sia stato posto in essere utilizzando mezzi tecnologici o la rete non comporta l'inapplicabilità della fattispecie di truffa comune[50]. Gli artifici e i raggiri ben possono essere commessi utilizzando il *web*, basti pensare alle finte fotografie di un finto prodotto falsamente posto in vendita su un sito di *e-commerce*, o ai raggiri coi quali il truffatore cerca di convincere la vittima che il suo schema Ponzi è un investimento molto redditizio[51].

A tal proposito, la giurisprudenza ha in più occasioni ritenuto che integra il reato di truffa contrattuale la condotta di colui che pone in vendita un bene su un sito di *e-commerce*, ricevendo il corrispettivo per la sua vendita, senza poi procedere alla consegna dello stesso e rendendo difficile la possibilità di risalire alla propria identità[52]. In particolare, la Cassazione ha evidenziato che l'indicazione di un falso luogo di residenza del venditore[53] o il rendersi irreperibile subito dopo la ricezione del corrispettivo[54] sono condotte che integrano il reato di truffa, posto che tali circostanze, rendendo difficile il rintraccio, evidenziano sintomaticamente la presenza del dolo iniziale del reato, da ravvisarsi nella volontà di non adempiere all'esecuzione del contratto sin dal momento dell'offerta *online*. La Suprema Corte ha poi ritenuto che pure la vendita *online* di un medesimo oggetto su due

[50] FLOR R., *La legge penale nello spazio*, cit., p. 162.
[51] In tal senso anche CIPOLLA P., *E-commerce e truffa*, cit., p. 2632, secondo cui «*si deve concludere dunque che il solo fatto dell'offrire in vendita una merce che non si possiede (e non si può né si vuole procurare in breve termine), per il tramite di strutture professionalmente preposte al commercio on line, costituisce certamente «raggiro», pur in assenza di esposizioni palesemente fallaci*».
[52] Cass. pen., sez. VI, sentenza 17 febbraio 2015, n. 10136.
[53] Cass. pen., sez. II, sentenza 19 luglio 2016, n. 43660.
[54] Cass. pen., sez. II, sentenza 2 marzo 2017, n. 18821.

siti differenti a due distinti acquirenti senza procedere all'invio dell'oggetto dopo il pagamento del corrispettivo costituisca truffa contrattuale, dato che tale circostanza costituisce la dimostrazione dell'intento truffaldino[55].

In altri casi ancora, ha ritenuto sussistente la truffa contrattuale, evidenziando che nel caso di vendita *online* gli artifici e raggiri consistono nella registrazione presso un portale di vendite, nella pubblicazione dell'annuncio unito alla descrizione del bene e nell'indicazione di un prezzo conveniente ovvero comunque appetibile, trattandosi di fattori tesi a carpire la buona fede dell'acquirente ed a trarre in inganno il medesimo[56]. In particolare, ha evidenziato che le vendite *online* si fondano sull'affidamento del compratore nella serietà dell'offerta del venditore, dato che l'acquirente non può vedere la merce che acquista e si affida integralmente per l'indicazione delle caratteristiche, delle qualità del prodotto e del prezzo di vendita alle indicazioni che vengono pubblicizzate dal venditore. Ciò determina la natura di artificio e raggiro della messa in vendita di un oggetto ad un prezzo appetibile per il mercato e senza che la successiva mancata consegna sia dovuta a specifici fattori intervenuti ed adeguatamente esposti dal venditore, in cui lo stesso ometta anche la dovuta restituzione del prezzo, trattandosi di condotta che stigmatizza la presenza del dolo iniziale di truffa[57].

Si evidenzia, però, la necessità di distinguere il mero inadempimento contrattuale dalla truffa *online*[58]. In questo caso, infatti, si è portati a ritenere che qualsiasi mancato invio della merce pubblicizzata su un sito *web* integri automaticamente gli estremi dell'art. 640 c.p. Ma il fatto che la vendita avvenga utilizzando il mezzo di *Internet* non significa affatto che non possa trattarsi di mero inadempimento contrattuale, come peraltro avviene nel mondo reale. Dunque, anche in tale ambito diviene indispensabile distinguere gli inadempimenti penalmente irrilevanti dalle condotte fraudolente. Infatti, non è sufficiente il mero mancato invio della merce, ma è necessaria la presenza di ulteriori circostanze che dimostrino in modo inequivoco la volontà truffaldina del venditore.

Va poi ribadito che nella compravendita di beni su *Internet* le parti non hanno contatti diretti e che in alcuni siti di *e-commerce* si richiede che il compratore paghi la merce anticipatamente, prima dell'effettivo invio della stessa. Questo pone l'acquirente in una situazione di debolezza, di cui spesso si approfittano i truffatori, che costruiscono finti

[55] Cass. pen., sez. II, sentenza 30 maggio 2022, n. 21038.
[56] Cass. pen., sez. II, sentenza 15 giugno 2022, n. 23323. In senso conforme anche Cass. pen., sez. II, sentenza 6 novembre 2019, n. 45115.
[57] *Ibid*.
[58] Necessità sottolineata anche da PARODI C., *Reati patrimoniali*, in *Diritto penale dell'informatica*, cit., p. 117.

annunci di vendita relativi a beni inesistenti o comunque che non hanno nessuna intenzione di alienare. Si deve, pertanto, esaminare la configurabilità in tali casi della circostanza aggravante della minorata difesa, richiamata al n. 2-*bis* del co. 2 dell'art. 640 c.p., in particolare in relazione alla diversità di ruolo, data la "distanza" tra il luogo di commissione del reato, ove si trova l'agente, e quello in cui si trova l'acquirente del bene *online*.

La giurisprudenza ha ritenuto applicabile l'aggravante in questione alle truffe contrattuali commesse attraverso siti di *e-commerce*, evidenziando che in questo caso la condotta fraudolenta è caratterizzata da particolari modalità, in specie la distanza tra venditore e acquirente, nonché l'offerta virtuale del bene, che viene venduto senza essere controllato. Dunque, l'aggravante della minorata difesa ben può essere riconosciuta, dato che le contrattazioni *online*, in ragione della distanza tra i contraenti, dell'impossibilità di potere effettuare controlli sui beni offerti in vendita e della facilità con cui il venditore può schermare la sua identità, pongono il compratore in una condizione di minorata difesa[59].

Anche in questo caso la dottrina ha respinto la teoria vittimo-dogmatica, evidenziando che la circostanza aggravante in questione non può affatto essere esclusa per il solo fatto che la vittima, scegliendo di comprare un bene *online*, si è volontariamente esposta ai rischi insiti in tale tipo di transazioni, dato che per giurisprudenza consolidata ai fini della sussistenza del reato di truffa la mancata diligenza della vittima non esclude l'idoneità degli artifici e raggiri, senza dimenticare la progressiva diffusione di tali mezzi[60].

Non tutti, però, sono d'accordo sul riconoscimento della circostanza aggravante in questione nelle vendite *online*. A tal proposito, vi è chi evidenzia che la "distanza" tra acquirente e finto venditore è in realtà elemento costitutivo delle truffe contrattuali commesse sul *web*, non una circostanza del reato[61]. Va però evidenziato che la stessa giurisprudenza della Suprema Corte ha escluso che la circostanza aggravante in questione si applichi ad ogni caso di vendita *online*. Infatti, l'ha ritenuta non applicabile in quei casi in cui la trattativa abbia preso avvio dall'ostensione di un bene su una piattaforma telematica, ma poi si sia sviluppata attraverso contatti telefonici e incontri in presenza. Ciò perché in

[59] Cass. pen., sez. II, sentenza 13 aprile 2022, n.18252. In senso conforme Cass. pen., sez. II, sentenza 14 dicembre 2021, n. 2902; Cass. pen., sez. VI, sentenza 22 marzo 2017, n. 17937; Cass. pen., sez. II, sentenza 29 settembre 2016, n. 43706.
[60] PARODI C., *Reati patrimoniali*, in *Diritto penale dell'informatica*, cit., p. 120.
[61] LEPERA M., *Un caso di reato semplice scambiato per reato circostanziato: sull'improbabile configurabilità dell'aggravante della "minorata difesa" in relazione alle truffe on-line*, in *Cass. Pen.*, 2017, n. 2, p. 687 ss., p. 693 s.

questi casi i contraenti non si trovano in condizione di minorata difesa, dato che hanno la possibilità di interagire direttamente con l'altro contraente[62].

È però evidente che al di fuori di questi casi specifici, in cui il mezzo *Internet* ha solo la funzione di mettere in contatto i potenziali contraenti, la circostanza aggravante in questione trova applicazione nella totalità dei restanti casi. Ciò è sintomo del fatto che le truffe commesse attraverso il *web* vengono percepite come "diverse" rispetto a quelle tradizionali, meritevoli di una sanzione penale più elevata rispetto a quelle comuni e, dunque, denota un'insoddisfazione di fondo per la struttura, e il trattamento sanzionatorio, della fattispecie di truffa comune, che non viene ritenuta idonea a sanzionare condotte connotate da questo particolare disvalore.

Come sopra evidenziato (v. *supra*, cap. I, par. 5), spesso in questo tipo di truffe i criminali utilizzano false generalità oppure si fingono altre persone realmente esistenti, utilizzando il loro nome, le loro fotografie ecc., magari aprendo falsi profili su *social network*. Si è esaminato in precedenza che tale comportamento integra anche il reato di sostituzione di persona di cui all'art. 494 c.p. (v. *supra*, cap. II, par. 7). A tal proposito, per giurisprudenza unanime il reato di sostituzione di persona può concorrere formalmente con quello di truffa, stante la diversità dei beni giuridici protetti, consistenti rispettivamente nella fede pubblica e nel patrimonio[63].

1.3. L'individuazione del *locus commissi delicti*

Si è visto, dunque, che anche i nuovi comportamenti truffaldini commessi attraverso la rete possono integrare il tradizionale reato di truffa. Tuttavia, il fatto che le frodi siano commesse attraverso l'utilizzo della rete pone problemi applicativi del tutto nuovi, in particolare quello relativo all'individuazione del *locus commissi delicti*. Come sopra evidenziato, la truffa è reato di evento che si consuma nel momento in cui alla condotta tipica faccia seguito la *deminutio patrimonii* del soggetto passivo. Infatti, come le trattative si svolgono interamente *online*, anche il pagamento avviene tramite strumenti di pagamento elettronici, quali accredito su carta *Postepay*, bonifico bancario, utilizzo di sistemi di pagamento quali *Moneytransfer*, *PayPal*, ecc. Non essendovi la dazione fisica del denaro da parte della vittima, in un luogo fisicamente determinato, si pone il problema di individuare

[62] Cass. pen., sez. II, sentenza 13 gennaio 2021, n. 1086. In senso conforme anche Cass. pen., sez. VI, sentenza 22 aprile 2017, n. 17937.
[63] V. *ex multis* Cass. pen., sez. II, sentenza 11 settembre 2020, n. 26589; Cass. pen., Sez. VI, sentenza 10 marzo 2010, n. 9470; Cass. pen., sez. II, sentenza 6 luglio 2007, n. 35443.

il *locus commissi delicti*, estremamente rilevante ai fini della determinazione e persecuzione del giudice competente sul commesso reato.

Nel caso in cui la vittima abbia effettuato il pagamento dei beni mai ricevuti attraverso la ricarica di una carta *Postepay* non abbinata ad un conto corrente, seguendo i principi generali sopra esposti in materia di truffa, per cui il reato in questione si consuma soltanto con l'effettivo conseguimento del bene e la perdita definitiva dello stesso da parte della vittima, dovrebbe ritenersi che il reato si consumi nel luogo in cui avviene l'incasso o è accettata la disposizione patrimoniale. Tuttavia, va evidenziato che la carta *Postepay* non solo non è necessariamente abbinata ad un conto corrente, ma può essere utilizzata presso qualsiasi ufficio postale, sportello automatico e anche *online*[64]. Dunque, come evidenziato da alcuni autori, in questo caso, poiché ad essere oggetto di ricarica è la stessa carta, il luogo del conseguimento del profitto finisce per coincidere con quello in cui la stessa viene utilizzata, ovvero uno dei molteplici sportelli ATM, o, addirittura, sul sito *Internet* nel quale viene utilizzata[65]. In questo modo diviene impossibile individuare il luogo "fisico" di conseguimento dell'ingiusto profitto ed ai fini dell'individuazione della competenza territoriale bisogna per forza fare riferimento ai criteri residuali di cui all'art. 9 c.p.p., in particolare quello della residenza, dimora o domicilio dell'imputato.

Per l'orientamento giurisprudenziale prevalente, dunque, il tempo e il luogo di consumazione del reato sono quelli in cui la persona offesa ha proceduto al versamento del denaro sulla carta, poiché tale operazione ha realizzato contestualmente sia l'effettivo conseguimento del bene da parte dell'agente, che ottiene l'immediata disponibilità della somma versata, e non un mero diritto di credito, sia la definitiva perdita dello stesso bene da parte della vittima[66]. Questo orientamento appare assolutamente coerente, nonché più aderente alla struttura della fattispecie, dato che nel momento in cui la persona offesa procede al versamento del denaro sulla carta tale operazione realizza contestualmente sia l'ingiusto profitto da parte dell'agente, sia la definitiva diminuzione patrimoniale in danno della vittima[67]. In questi casi non vi sono ostacoli nel ritenere che il momento consumativo della truffa possa coincidere con il compimento dell'atto di disposizione patrimoniale[68].

[64] V. il funzionamento della carta sul sito https://postepay.poste.it.
[65] PECORELLA C., *Truffe on-line: momento consumativo e competenza territoriale*, in *Riv. it. dir. proc. pen*., 2012, n. 1, p. 113 ss., p. 114.
[66] Cass. pen., sez. II, sentenza 17 luglio 2020, n. 23781; Cass. pen., sez. II, sentenza 6 giugno 2019, n. 49195; Cass. pen., sez. II, sentenza 10 gennaio 2017, n. 14730; Cass. pen., sez. I, sentenza 13 marzo 2015, n. 25230.
[67] Della stessa opinione anche FLOR R., *La legge penale nello spazio*, cit., p. 167.
[68] In tal senso già PEDRAZZI C., *Postilla circa la competenza per territorio in materia di truffa*, in *Riv. It. Dir. proc. pen*., ora anche in PEDRAZZI C., *Scritti di diritto penale*. *Vol. II scritti di parte speciale*, Milano, 2003, p. 359 ss., p. 361 ss.

Infatti, dato che la disposizione non è revocabile, in quel momento si verifica la definitiva perdita della somma da parte del soggetto passivo, assieme al suo effettivo conseguimento da parte dell'agente.

Tale soluzione, però, mal si adatta ai casi in cui l'atto di disposizione patrimoniale sia revocabile, nei quali la vittima, nonostante abbia eseguito il bonifico, una volta accortasi della truffa abbia la possibilità di revocare la disposizione effettuata ed annullare l'accredito della somma di denaro. Qui, infatti, la disposizione patrimoniale non corrisponde alla definitiva perdita della somma da parte del correntista. La stessa giurisprudenza della Cassazione adotta una soluzione diversa da quella da ultimo descritta qualora il pagamento sia effettuato tramite bonifico bancario. In questo caso, infatti, ritiene che la truffa si consumi nel luogo ove l'agente consegue l'ingiusto profitto tramite la riscossione della somma e non già in quello in cui viene data la disposizione per il pagamento da parte della persona offesa[69]. Viene infatti evidenziato che se ad essere utilizzato è un sistema di pagamento di tipo telematico, come il bonifico bancario *online*, non vi è immediata e contestuale coincidenza tra spoliazione per il disponente che lo esegue e il contestuale arricchimento per il soggetto agente, giacché l'autore del bonifico conserva il potere di revocare la disposizione fino alla scadenza del termine determinato dalla banca[70].

Se il conto corrente è aperto in una determinata filiale fisica non vi sono particolari problemi di individuazione del luogo del commesso reato, che coincide con quello in cui si trova la filiale. Tuttavia, essi si pongono qualora si tratti di una banca operante solo nel *web*. In questo caso, ai fini della determinazione della competenza territoriale, si può fare riferimento unicamente ai criteri residuali di cui all'art. 9 c.p.p., data l'impossibilità di individuare un luogo fisico in cui è stata accreditata la somma[71].

Il problema relativo all'individuazione del *tempus* e del *locus commissi delicti* non riguarda solo le truffe commesse *online*, ma le anche altre tradizionali fattispecie poste a tutela del patrimonio, quale l'estorsione. Anche tale ultimo reato, infatti, esattamente come la truffa si presta ad una realizzazione cibernetica, che viene comunemente denominata estorsione *online* o cyberestorsione[72].

---

[69] Cass. pen., sez. II, sentenza 2 dicembre 2019, n. 48987; Cass. pen., sez. II, sentenza 7 dicembre 2017, n. 54948; Cass. pen., sez. II, sentenza 20 febbraio 2015, n. 7749.
[70] Cass. pen., sez. I, sentenza 1 aprile 2021, n. 21357.
[71] FLOR R., *La legge penale nello spazio*, cit., p. 167.
[72] LUBERTO M., "Sex-torsion" *via* web *e minaccia a mezzo* ransomware, cit., p. 726.

1.4. L'estorsione

L'estorsione appartiene alla categoria dei delitti con cooperazione artificiosa della vittima: anch'essa si incentra sull'atto di disposizione patrimoniale, effetto della collaborazione della vittima non puramente meccanica, ma cosciente e volontaria, anche se dovuta alla minaccia[73]. Trattasi di reato plurioffensivo, che tutela sia il patrimonio che la libertà morale del soggetto passivo[74]. Soggetto passivo può essere sia colui contro il quale viene realizzata la violenza o minaccia, sia un'altra persona se, per effetto di essa, subendo l'intimidazione, si induca ad un atto per lei pregiudizievole. Non vi è quindi necessaria identità tra il minacciato, l'intimidito e il danneggiato. Si è però rilevato che in tale ipotesi la *vis*, ancorché diretta materialmente verso altra persona, è pur sempre usata per coartare la volontà del titolare dell'interesse patrimoniale leso che deve essere indotto a compiere l'atto dispositivo, sicché anche in questo caso il soggetto passivo del reato è pure soggetto passivo della condotta[75]. Soggetto passivo può essere anche una persona giuridica quando il fatto avvenga mediante minaccia[76].

La condotta consiste nella coartazione commessa mediante violenza o minaccia. Trattasi quindi, di reato a forma vincolata[77], nel quale la violenza consiste in qualsiasi attività fisica volta ad indurre il destinatario ad effettuare la disposizione patrimoniale, mentre nel concetto di minaccia rientra qualsiasi prospettazione di un male futuro presentato come dipendente dall'agente[78]. La costrizione può essere realizzata sia con un'azione che con un'omissione, ma è necessario che l'oggetto materiale dell'azione od omissione consista in un atto capace d'incidere in modo diretto o indiretto sul patrimonio del soggetto passivo[79].

Per quanto riguarda la violenza, oggi è pacificamente ammesso che la stessa possa essere esercitata anche sulle cose e non debba essere necessariamente rivolta alle persone, dato che l'art. 629 c.p., a differenza che per la rapina, fa unicamente riferimento alla nozione di "violenza"[80]. Si evidenzia, inoltre, che ben può ottenersi la coazione psichica mediante il danneggiamento di cose, attraverso la c.d. violenza reale descritta dall'art. 392 c.p.[81] La violenza reale può configurarsi dunque anche come violenza "informatica", dato che il

[73] LAURINO A., *L'estorsione*, in F. Viganò, C. Piergallini (a cura di), *Reati contro la persona e contro il patrimonio*, Torino, 2015, p. 499 ss., p. 499.
[74] BARAZZETTA A., *Sub art. 629 c.p.*, in *Commentario breve al Codice penale*, cit., p. 2200 ss., p. 2200.
[75] BARAZZETTA A., *Sub art. 629 c.p.*, cit., p. 2201. In giurisprudenza v. Cass. pen., sez. I, sentenza 28 maggio 2014, n. 25382.
[76] CONTI L., voce *Estorsione*, in *Enc. Dir*., vol. XV, Milano, 1966, p. 995 ss., p. 997.
[77] LUBERTO M., "Sex-torsion" *via* web *e minaccia a mezzo* ransomware, cit., p. 733.
[78] MARINI G., voce *Estorsione*, in *Dig. disc. pen.*, vol. IV, Torino, 1992, p. 377 ss., p. 381.
[79] CONTI L., voce *Estorsione*, cit., p. 999.
[80] *Ibid*., p. 997.
[81] LAURINO A., *L'estorsione*, cit., p. 501.

disposto dell'art. 392 ultimo co. equipara la violenza sui programmi e sui sistemi informatici alla "violenza sulle cose"[82].

Con riferimento alla minaccia, la Cassazione reputa indifferente la forma e il modo della minaccia, per cui la stessa può essere oltre che esplicita, palese e determinata, anche manifestata in maniera indiretta, ovvero implicita e indeterminata, basta che sia idonea ad incutere timore e a coartare la volontà del soggetto passivo in relazione alle circostanze concrete, alla personalità della vittima, alle sue condizioni soggettive ed alle condizioni ambientali in cui opera l'agente[83]. A tal proposito, ha ritenuto costituisca minaccia rilevante ai sensi dell'art. 629 c.p. anche quella di interrompere un legame affettivo o l'affiliazione della vittima ad un gruppo amicale, evidenziando che la stessa può assumere rilievo come strumento di coazione per l'ottenimento di un ingiusto profitto in ragione della particolare condizione di debolezza della vittima che la induca a collegare all'evento minacciato conseguenze deteriori del tutto esorbitanti dal dolore normalmente collegato all'abbandono o al tradimento, e della consapevole strumentalizzazione di tale condizione di debolezza da parte dell'agente[84].

La condotta dev'essere diretta a provocare gli eventi descritti nella norma, ovvero il conseguimento dell'ingiusto profitto con altrui danno, tramite la causazione di una condizione di timore[85]. Anche in questo caso l'elemento dell'ingiusto profitto è stato individuato in qualsiasi vantaggio, non solo di tipo economico, che l'autore intenda conseguire e che non si collega a un diritto, ovvero è perseguito con uno strumento antigiuridico o con uno strumento legale ma avente uno scopo tipico diverso[86]. Diversamente, il danno deve necessariamente avere carattere patrimoniale, anche se è indifferente che l'oggetto della minaccia sia o non sia il patrimonio o che lo scopo del profitto sia o meno la realizzazione di un vantaggio economico[87].

Anche l'estorsione è reato di evento, che si consuma nel momento in cui il reo consegue l'ingiusto profitto e la vittima subisce il danno patrimoniale[88].

---

[82] LUBERTO M., "Sex-torsion" *via* web *e minaccia a mezzo* ransomware, cit., p. 727. V. anche PICOTTI L., *Sistematica*, cit., p. 35 s. e 49 ss.
[83] Cass. pen., sez. II, sentenza 21 gennaio 2016, n. 2702; Cass. pen., sez. II, sentenza 14 marzo 2013, n. 11922; Cass. pen., sez. II, sentenza 18 gennaio 2013, n. 2833; Cass. pen., sez. II, sentenza 19 giugno 2012, n. 36698.
[84] Cass. pen., sez. II, sentenza 12 luglio 2007, n. 35484.
[85] MARINI G., voce *Estorsione*, cit., p. 384.
[86] SALVINI A., voce *Estorsione e sequestro di persona a scopo di rapina o di estorsione*, in *Noviss. Dig. It.*, vol. VI, Torino, 1960, p. 1000 ss., p. 1003; Cass. pen., sez. II, sentenza 31 marzo 2008, n. 16658.
[87] CONTI L., voce *Estorsione*, cit., p. 1000.
[88] *Ibid*.

Elemento soggettivo è il dolo generico[89]. Si evidenzia, infatti, che il fine di procurare a sé o ad altri un ingiusto profitto non attiene all'elemento psichico del reato, visto che ne costituisce l'evento[90].

Non sempre è facile distinguere tra truffa ed estorsione. Entrambe le fattispecie, infatti, richiedono l'atto di disposizione patrimoniale della vittima. La differenza, però, risiede nella genesi causale di tale atto: infatti, nella truffa essa deriva da un artificio o un raggiro del reo, nell'estorsione da una violenza o da una minaccia[91]. Nella truffa la persona offesa si determina alla consegna della cosa in quanto i mezzi fraudolenti utilizzati dall'agente hanno formato in lui l'erroneo convincimento di dover consegnare la cosa, mentre nell'estorsione la determinazione è dovuta al timore di subire un maggior danno e dalla speranza di poterlo in qualche modo evitare[92]. Per quanto riguarda, invece, la differenza tra la truffa aggravata di cui all'art. 640 co. 2 n. 2 c.p. e l'estorsione, si ritiene che la distinzione risieda nel contenuto del messaggio intimidatorio, per cui nell'estorsione il colpevole incute il timore di un danno che fa apparire come certo e proveniente da lui o da altra persona in rapporto con lui, per cui la persona offesa, posta nell'alternativa di ottemperare a quanto richiestole ovvero di subire un danno patrimoniale, viene coartata nella sua volontà. Diversamente, nel caso della truffa aggravata il colpevole suscita nella vittima l'immaginario pericolo di un danno futuro da lui però non dipendente né direttamente, né indirettamente, per cui la vittima si determina alla condotta unicamente per effetto dell'errore nel quale è caduta, non perché coartata[93].

Nell'ambito applicativo della fattispecie di estorsione possono dunque rientrare tutte quelle condotte nelle quali i criminali minacciano via *mail* o via *chat* la vittima per indurla a compiere una determinata disposizione patrimoniale[94]. Posto che, come evidenziato, il futuro male prospettato non deve avere necessariamente carattere patrimoniale, può rientrare nell'ambito applicativo della norma anche il fenomeno della *sextortion*, che si configura

[89] ANGELOTTI D., *Delitti contro il patrimonio*, cit., p. 306; CONTI L., voce *Estorsione*, cit., p. 1001; MARINI G., voce *Estorsione*, cit., p. 387.
[90] SALVINI A., voce *Estorsione e sequestro di persona*, cit., p. 1004.
[91] LUCARELLI U., *La truffa*, cit., p. 44.
[92] SALVINI A., voce *Estorsione e sequestro di persona*, cit., p. 1004.
[93] LUCARELLI U., *La truffa*, cit., p. 214; ZANNOTTI R., *La truffa*, cit., p. 135. In giurisprudenza v. Cass. pen., sez. II, 1 settembre 2020, n. 24624; Cass. pen., sez. II, 2 febbraio 2018, n. 5092; Cass. pen., sez. II, 2 gennaio 2017, n. 5; Cass. pen., sez. II, sentenza 15 giugno 2016, n. 44942; Cass. pen., sez. II, sentenza 17 febbraio 2016, n. 11453; Cass. pen., sez. II, sentenza 21 ottobre 2015, n. 46084; Cass. pen., sez. II, sentenza 25 novembre 2014, n. 52121; Cass. pen., sez. II, sentenza 6 maggio 2014, n. 20656; Cass. pen., sez. II, sentenza 30 giugno 2010, n. 35346.
[94] SCOPINARO L., *Internet e reati contro il patrimonio*, Torino, 2007, p. 190 ss. In tal senso anche Cass. pen., sez. II, sentenza 12 dicembre 2012, n. 11922.

qualora il reo intimi alla vittima di consegnargli del denaro in cambio della mancata divulgazione delle immagini a contenuto pornografico[95]. È però necessario che la richiesta dell'agente sia diretta a far compiere alla vittima un atto di disposizione patrimoniale, dato che la norma richiede espressamente un danno economico. Pertanto, tutti quei casi in cui la richiesta dell'agente non abbia un contenuto apprezzabilmente patrimoniale, quale ad esempio la richiesta di invio di immagini a sfondo sessuale o il compimento di atti sessuali, non potrà esservi estorsione ai sensi dell'art. 629 c.p., ma potrà configurarsi un diverso reato quale ad esempio violenza privata o violenza sessuale[96].

L'estorsione può essere realizzata tramite *ransomware* ovvero mediante il lancio di un *malware* per ottenere un riscatto, sia in moneta elettronica che in criptovalute[97]. Come sopra evidenziato, infatti, il reato di estorsione può essere commesso anche mediante violenza c.d. informatica. L'art. 392 co. 3 c.p., però, specifica che si ha violenza sulle cose «*allorché un programma informatico viene alterato, modificato o cancellato in tutto o in parte ovvero viene impedito o turbato il funzionamento di un sistema informatico o telematico*». Occorre, pertanto, operare un distinguo. Nel caso in cui il *ransomware* abbia disattivato le opzioni di avvio/blocco del sistema compromettendone le funzionalità è configurabile la violenza informatica. Qualora, invece, il virus sia intervenuto unicamente sui dati ed informazioni rendendoli inaccessibili non sembra potersi configurare la "violenza informatica", dato che la norma fa riferimento unicamente a sistemi e programmi[98]. Tuttavia, va evidenziato che all'atto pratico difficilmente il *ransomware* si limita ad agire su singoli dati e informazioni, coinvolgendo piuttosto intere cartelle di *file*, le quali possono essere ricomprese nella nozione di programmi informatici.

Un problema di identificazione della fattispecie può porsi con riferimento a quei *ransomware* in cui, nella richiesta di riscatto, i criminali informatici affermano falsamente di essere appartenenti alle Forze dell'ordine. L'affermare falsamente di essere appartenente ad un corpo di Polizia, infatti, può costituire un artificio o un raggiro, per cui si pone il problema dell'astratta configurabilità dell'art. 640 c.p., in questo caso aggravato dall'aver ingenerato nella persona offesa il timore di un pericolo immaginario o l'erroneo convincimento di dovere eseguire un ordine dell'Autorità. Però in questo caso il timore è effetto di una minaccia, che ha la conseguenza di limitare la libertà del volere. Qui, infatti,

[95] LUBERTO M., "Sex-torsion" *via* web *e minaccia a mezzo* ransomware, cit., p. 737.
[96] Ibid., p. 740.
[97] BRIZZI F., *I profili penali del ransomware*, in *Il processo telematico*, 21 febbraio 2002, p. 7, disponibile *online* all'indirizzo ilprocessotelematico.it.
[98] LUBERTO M., "Sex-torsion" *via* web *e minaccia a mezzo* ransomware, cit., p. 736.

il soggetto passivo è indotto a compiere l'atto pregiudizievole non perché ingannato, ma perché vi è una vera e propria coazione del volere che esclude la sua libertà, dato che è impedito nell'utilizzo del suo dispositivo elettronico dall'esecuzione del *ransomware*. Già in passato si è qualificata come estorsione la condotta di falsi agenti di Polizia che allegavano vere o pretese violazioni di legge si facevano così consegnare somme di denaro per evitare la denuncia o l'arresto. Questo perché in tal caso l'artificio cui il legislatore si riferisce non può considerarsi un semplice mezzo fraudolento, ma costituisce un vero e proprio mezzo di coercizione sul soggetto passivo[99]. Pertanto, nel caso sopra descritto si deve concludere per la sussistenza del reato di estorsione, non di truffa aggravata.

2. La frode informatica *ex* art. 640-*ter* c.p. e i suoi ambiti applicativi

Il delitto di frode informatica è stato inserito nel nostro ordinamento dall'art. 10 della citata l. 23 dicembre 1993 n. 547 allo scopo di risolvere la difficoltà di ricondurre le condotte fraudolente poste in essere mediante sistemi informatici nella fattispecie di truffa, dato che, in virtù del divieto di analogia *in malam partem,* non si riteneva possibile assimilare l'impiego fraudolento della macchina all'inganno di un uomo[100]. L'art. 640 c.p. veniva infatti applicato dalla giurisprudenza nei soli casi di manipolazioni di dati ove vi era stata una qualche tipologia d'intervento anche da parte della persona utilizzatrice. Tale norma, pertanto, non era ritenuta idonea a sanzionare tutti quei comportamenti ingannevoli posti in essere nei confronti di un elaboratore elettronico[101].

Dunque, in linea con le raccomandazioni del Consiglio d'Europa, il nostro legislatore ha introdotto una norma *ad hoc* per punire la frode informatica, collocandola tra i delitti contro il patrimonio. Essa punisce le condotte fraudolente che incidono sul funzionamento di un sistema informatico o sul contenuto di dati informatici. In altre parole, le note modali degli artifizi e raggiri, che caratterizzano il delitto tradizionale di truffa, vengono sostituite dalla condotta tipica della manipolazione di dati e di sistemi informatici, che mal si prestava a rientrare nella fattispecie generale della truffa comune[102]. La stessa denominazione di "frode" in luogo di "truffa" evidenzia la sussistenza di un'oggettiva idoneità ingannevole

[99] SALVINI A., voce *Estorsione e sequestro di persona*, cit., p. 1005.
[100] FINOCCHIARO G., *Diritto di Internet*, Bologna, 2008, p. 224; PICA G., *Diritto penale delle tecnologie informatiche*, cit., p. 140.
[101] Cft. MARINI G., *voce Truffa,* cit., p. 869, secondo cui «*deve subito dirsi che destinatario degli artifici o raggiri può solo essere una persona fisica, in quanto tale o in quanto titolare di un organo pubblico o privato. Il problema dell'ammissibilità della cosiddetta truffa realizzata "ingannando" gli apparecchi automatici, pertanto, deve essere risolto […] negativamente*». Così anche ZANNOTTI R., *La truffa*, cit., p. 60.
[102] PICOTTI L., *Sistematica*, cit., p. 51; FINOCCHIARO G., *Diritto di Internet*, cit., p. 54.

dell'azione, in quanto attuata attraverso la manipolazione dei sistemi informatici, alterandone il funzionamento secondo logiche coerenti con le intenzioni di illecito profitto dell'agente, ma diverse da quelle volute dal legittimo titolare e/o utilizzatore del sistema e all'insaputa di questi[103]. Ciò giustifica la denominazione differente rispetto a quella di truffa, imperniata invece sull'induzione in errore della vittima.

Come risulta quindi dalla sua collocazione, ritenuta senz'altro appropriata[104], il bene giuridico tutelato dalla norma è il patrimonio[105]. Scopo principale della fattispecie è di reprimere le ipotesi di illecito arricchimento conseguite attraverso l'utilizzo fraudolento di un sistema informatico e l'alterazione di dati informatici. Secondo una parte della dottrina oggetto della tutela è anche la regolarità di funzionamento di detti sistemi e della riservatezza che accompagna l'utilizzatore[106].

La norma punisce, con la reclusione da sei mesi a tre anni, «*chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno*». Come si può notare, la struttura normativa del delitto in esame è in parte analoga a quella della truffa tradizionale. Per questo motivo, alcuni autori ritengono che la frode informatica non sia che un'ipotesi speciale di truffa[107]. A tal proposito, la Cassazione ha precisato in più occasioni che il reato di frode informatica si differenzia da quello di truffa unicamente perché l'attività fraudolenta dell'agente non investe una persona, bensì il sistema informatico, attraverso la manipolazione di detto sistema[108].

Tuttavia, va evidenziato che nella frode informatica non è richiesta alcuna

[103] PICA G., *Diritto penale delle tecnologie informatiche*, cit., p. 143.
[104] PICOTTI L., *Sistematica dei reati informatici*, cit., p. 54.
[105] MANNA A., *Artifici e raggiri on-line: la truffa contrattuale, il falso informatico e l'abuso dei mezzi di pagamento elettronici*, in *Dir. inf. inf*., 2002, n. 6, p. 955 ss., p. 965; MINICUCCI G., *Le frodi informatiche*, in *Cybercrime*, cit., p. 827 ss., p. 829.
[106] FIANDACA G., MUSCO E., *Diritto penale. PS*, cit., p. 209; PICOTTI L., *Sistematica dei reati informatici*, cit., p. 55; MARGIOCCO M., *Frode informatica*, in G. Finocchiaro, F. Delfini, *Diritto dell'informatica*, Milano, 2014, p. 1107 ss., p. 1108.
[107] PICA G., *Diritto penale delle tecnologie informatiche*, cit., p. 141.
[108] «*Il reato di frode informatica (art. 640 ter c.p.) ha la medesima struttura e quindi i medesimi elementi costitutivi della truffa dalla quale si differenzia solamente perché l'attività fraudolenta dell'agente investe non la persona (soggetto passivo), di cui difetta l'induzione in errore, bensì il sistema informatico di pertinenza della medesima, attraverso la manipolazione di detto sistema. Anche la frode informatica si consuma nel momento in cui l'agente consegue l'ingiusto profitto con correlativo danno patrimoniale altrui*» Cass. pen., sez. VI, sentenza 4 ottobre 1999, n. 3065. Più di recente v. anche Cass. pen., sez. II, sentenza 10 febbraio 2020, n. 10534

collaborazione della vittima per raggiungere l'ingiusto profitto[109]. Infatti, il processo decisionale umano è integralmente sostituito dal trattamento di dati affidato all'elaboratore, cosa che non è priva di riflessi sul piano giuridico[110], perché tale caratteristica rende la frode informatica ontologicamente diversa dalla truffa comune, in cui la cooperazione della vittima è elemento essenziale della fattispecie. È evidente, pertanto, che la frode informatica non può essere considerata come mera ipotesi speciale di truffa, dato che presenta caratteristiche del tutto particolari che la allontanano dal modello della fattispecie tradizionale[111].

Il duplice evento tipico dell'ingiusto profitto con altrui danno è il medesimo della truffa comune, ma non vi è perfetta coincidenza tra le due fattispecie, in quanto mancano sia l'estremo dell'induzione in errore del soggetto passivo, sia gli artifici o raggiri, proprio perché entrambi i requisiti sono difficilmente configurabili se si opera sul *computer*[112].

Un settore della dottrina ritiene che l'elemento dell'induzione in errore della vittima, o causazione di un risultato inesatto o irregolare nel processo di elaborazione di dati rispetto al quale è intervenuta la manipolazione, vada ritenuto dall'interprete della norma in questione come requisito tacito[113]. In tal modo sarebbe assicurato al reato di cui all'art. 640-*ter* c.p. un ambito di operatività circoscritto ed uno sviluppo causale simmetrico a quello che già caratterizza la truffa. Altri, invece, ritengono che non si possa in alcun modo paragonare l'induzione in errore di un elaboratore elettronico con l'induzione in errore di una persona fisica[114]. Quest'ultima tesi è preferibile, in quanto un procedimento automatico di elaborazione dei dati non può essere in nessun modo paragonabile ad una decisione umana. Si può concordare, pertanto, con quegli autori che sostengono che in realtà la frode informatica non dovrebbe essere messa in relazione con la truffa, bensì col furto aggravato dal mezzo fraudolento, visto che in assenza dell'induzione in errore si prescinde completamente dalla cooperazione della vittima[115]. Tuttavia manca rispetto al furto il riferimento alla specifica *res* che è oggetto di conflitto tra autore e possessore legittimo.

Il fatto sanzionato dal legislatore consiste nell'alterare abusivamente il funzionamento di un sistema informatico o telematico altrui, oppure nell'intervenire senza

---

[109] BELLI M., *I delitti di truffa e frode informatica,* in *Reati contro la persona e contro il patrimonio*, cit., p. 701 ss., p. 701.
[110] PICOTTI L., *Sistematica dei reati informatici,* cit., p. 55.
[111] PECORELLA C., *Il diritto penale dell'informatica,* cit., p. 63; MINICUCCI G., *Le frodi informatiche,* cit., p. 828.
[112] FIANDACA G., MUSCO E., *Diritto penale parte speciale*, cit., p. 209.
[113] AMATO D., *Sub Art. 640-ter,* cit. p. 2280.
[114] MANNA A., *Artifici e raggiri on-line,* cit., p. 961.
[115] MANTOVANI F., *Diritto penale, PS,* cit., p. 217.

diritto su dati, informazioni o programmi contenuti nel sistema o ad esso pertinenti. La prima condotta consiste nella modifica del regolare svolgimento del processo di elaborazione o trasmissione dei dati realizzato da un sistema informatico[116], ossia in ogni attività o omissione che, attraverso la manipolazione dei dati informatici, incida sul regolare svolgimento del processo di elaborazione e/o trasmissione dei dati. La condotta fraudolenta dell'alterazione può avvenire in qualsiasi modo, agendo sul *software* ovvero sulla componente logica del *computer*, vale a dire su programmi, dati, informazioni installati e memorizzati in un apparato con capacità di elaborazione, oppure operando sull'*hardware*, cioè sulle parti elettroniche, meccaniche, magnetiche, ottiche che ne consentono il funzionamento, in modo tale da far compiere operazioni diverse rispetto a quelle per le quali la macchina è stata programmata (ad es. con un'azione volta a modificarne la componente *hardware*), dato che la norma prevede l'inciso «*in qualsiasi modo*»[117]. La nozione di alterazione è dunque talmente ampia che una parte della dottrina qualifica il reato in questione come reato a forma libera[118]. Pertanto, nella stessa possono senz'altro essere ricomprese le condotte di ostacolo o interferenza del sistema di informazione, nonché di introduzione, alterazione, cancellazione, trasmissione o soppressione di dati informatici, condotte che l'art. 6 della menzionata direttiva 2019/713/UE impone di sanzionare qualora siano commesse per arrecare illecitamente a terzi una perdita patrimoniale. È, pertanto, da accogliere con favore la scelta del legislatore italiano che, in sede di recepimento della suddetta direttiva, ha deciso di non aggiungere ulteriori condotte a quelle già sanzionate dall'art. 640-*ter* c.p., per cui la norma non risulta sovrabbondante.

Sulla portata del concetto di sistema informatico si sono sviluppate due teorie[119]: una prima, restrittiva, ritiene che per la fattispecie sia rilevante solo un complesso di apparecchiature e dispositivi dotato di un grado elevato di strutturazione e complessità: andrebbe dunque escluso il singolo *computer*. La seconda, invece, oggi prevalente, ritiene che sia un sistema informatico qualsiasi apparecchio che fornisca beni o servizi e che questi siano gestiti da un elaboratore; dunque, vi rientra anche il singolo dispositivo[120], nonché, secondo la giurisprudenza, anche la rete telefonica[121]. Per sistema telematico, invece, si

---

[116] PECORELLA C., *Il diritto penale dell'informatica,* cit., p. 82; Cass. pen., sez. II, 6 marzo 2013, n. 13475
[117] PECORELLA C., *Il diritto penale dell'informatica*, cit., p. 82;
[118] BELLI M., *I delitti di truffa e frode informatica,* cit., p. 703. In giurisprudenza v. Cass. pen., sez. II, sentenza 2 febbraio 2017, n. 9191;
[119] AMATO D., *Sub Art. 640-ter,* cit. p. 2279.
[120] MINICUCCI G., *Le frodi informatiche,* cit., p. 831; PECORELLA C., *Il diritto penale dell'informatica,* cit., p. 70.
[121] «*Poiché l'espressione "sistema informatico" di cui all'art. 640 ter c.p. si riferisce ad una pluralità di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo attraverso l'utilizzazione (anche*

intende qualsiasi rete di comunicazione gestita in via informatica[122].

Alla distinta ipotesi "*intervento senza diritto su dati, informazioni o programmi*" deve attribuirsi il significato di qualsiasi azione che produca un qualche effetto nel processo dell'elaboratore. Con questa formula si intende ogni forma di interferenza in un processo di elaborazione dei dati, trattandosi di una formulazione ampia idonea a ricomprendere tutte quelle ipotesi che già non rientrano nella condotta di alterazione[123]. Il suo elemento caratterizzante non è in sé manipolatorio, bensì normativo, perché non legittimo.

Per quanto riguarda i dati, essi sono intesi come le registrazioni elementari nella memoria di una macchina elaboratrice codificate in una forma non percettibile visivamente, ma che possono essere "letti", meglio trattati dall'elaboratore. Le informazioni sono invece intese come il contenuto del sistema informatico, costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consenta di attribuire loro un particolare significato per l'utente della macchina. I programmi informatici sono sequenze di istruzioni e l'intervento su di essi si compie facendo svolgere al *computer* operazioni in modo diverso da quelle legittimamente programmate. Queste nozioni sono utilizzate anche in altre norme (artt. 635-*bis* e 635-*ter* c.p.)[124].

L'intervento sul sistema informatico deve infatti essere "*senza diritto*". Alcuni autori ritengono che tale requisito debba essere interpretato come intervento realizzato da chi non è legittimato a farlo ed ha agito in modo arbitrario ed ingiustificabile[125]. Per altri autori, tuttavia, si tratterebbe di una specificazione inutile e superflua, dato che si tratta di un reato volto al conseguimento di un illecito accrescimento patrimoniale, per cui sarebbe del tutto irrilevante stabilire se l'agente abbia o meno il diritto di intervenire sui dati e sul *software*. Addirittura sarebbe una locuzione potenzialmente dannosa, dato che può comportare il rischio che venga interpretata come clausola di impunità per coloro che sono autorizzati ad operare sul sistema[126].

Analogamente all'alterazione del funzionamento del sistema, anche l'intervento senza

---

in parte) di tecnologie informatiche, deve ritenersi che sia la rete telefonica di cui si serve la Telecom, sia il centralino di una singola filiale costituiscono un sistema che si avvale di tecnologie informatiche»: così Cass. pen., sez. VI, 4 ottobre 1999, n. 3065, cit.

[122] MINICUCCI G., *Le frodi informatiche*, cit., p. 832.

[123] AMATO D., *Sub Art. 640-ter*, cit., p. 2279.

[124] SALVADORI I., *Il "microsistema" normativo concernente i reati informatici. Un bilancio molto poco esaltante*, in *Riv. it. dir. pen. proc.*, n. 1, 2012, p. 204 ss., p. 208 ss.

[125] Secondo Mantovani si tratta di «*un'ipotesi di antigiuridicità speciale non reale, ma apparente perché non fa che richiamarsi all'assenza della facoltà giuridica di agire, di cui all'art. 51*» v. MANTOVANI F., *Diritto penale*, *PS*, cit., p. 226.

[126] PICA G., *Diritto penale delle tecnologie informatiche*, cit., p. 147.

diritto può realizzarsi con qualsiasi modalità. Esso può consistere sia in un'alterazione o soppressione dei dati già contenuti nel sistema, sia nell'introduzione di dati falsi[127].

Un settore della dottrina ritiene che le condotte descritte nell'art. 640-*ter* c.p. in realtà non siano alternative tra loro, perché possono essere entrambe ricondotte all'alterazione, posto che l'intervento sui dati sarebbe soltanto un'operazione necessariamente preparatoria per riuscire ad influenzare il funzionamento della macchina[128]. Ma la giurisprudenza non è di quest'avviso, riconoscendo invece autonomia al concetto di intervento senza diritto rispetto a quello di alterazione[129].

L'art. 640-*ter* c.p. è un reato a duplice evento, come la truffa, costituito dall'altrui danno patrimoniale e dall'ingiusto profitto per l'agente o altri. Esso si consuma nel momento in cui per la vittima si verifica il danno patrimoniale e per l'agente l'ingiusto profitto. Se i due eventi non sono simultanei la fattispecie si consuma nel momento in cui si verifica l'ultimo evento del profitto[130]. Anche in questo caso si ritiene che per profitto possa intendersi qualsiasi utilità, anche di natura non patrimoniale[131]. Il danno, invece, deve necessariamente avere una connotazione economico-patrimoniale[132].

Si tratta di un reato comune perché soggetto attivo è "chiunque"[133]. Per quanto riguarda l'elemento soggettivo si tratta di fattispecie a dolo generico, richiedendo che il soggetto agisca con coscienza e volontà di realizzare le condotte tipizzate e tramite esse cagionare un altrui danno e ricavare un ingiusto profitto. Non è richiesta invece la volontà di indurre in errore[134], non essendo questo un elemento del fatto tipico.

A livello di trattamento sanzionatorio, la fattispecie base di frode informatica ha la stessa pena prevista per la truffa. Questa coincidenza, tuttavia, non è pienamente giustificabile. Infatti, la ragione della più forte punizione del furto rispetto alla truffa sta

---

[127] PECORELLA C., *Il diritto penale dell'informatica*, cit., p. 90; BELLI M., *I delitti di truffa e frode informatica*, cit., p. 710.

[128] PICA G., *Diritto penale delle tecnologie informatiche*, cit., p. 144, che evidenzia come l'alterazione costituirebbe la vera e unica modalità di commissione della frode informatica, mentre l'ulteriore condotta di intervento non sarebbe altro che un'azione preparatoria ed induttiva dell'alterazione del funzionamento, che in questa si evolve e si assorbe.

[129] «*Il reato ex art. 640-ter c.p. prevede due distinte condotte; la prima consiste nell'alterazione, in qualsiasi modo, del funzionamento di un sistema informatico o telematico; la seconda è rappresentata dall'intervento senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un dato sistema informativo o telematico. Tale ipotesi, finalizzata pur sempre all'ottenimento di un ingiusto profitto con altrui danno, si concretizza in un'illecita condotta intensiva ma non alterativa del predetto sistema*» in tal senso Cass. pen., sez. II, 6 marzo 2013, n. 13475, cit.

[130] MANTOVANI F., *Dir. pen.*, *PS*, cit., p. 226.

[131] PICA G., *Diritto penale delle tecnologie informatiche*, cit., p. 148.

[132] MINICUCCI G., *Le frodi informatiche*, cit., p. 836.

[133] BELLI M., *I delitti di truffa e frode informatica*, cit., 706.

[134] MANTOVANI F., *Dir. pen.*, *PS*, vol. II, IV ed., Padova, 2016, p. 226.

proprio nel fatto che nel primo caso l'attività del delinquente, posta in essere per vincere gli ostacoli di prevenzione disposti a tutela del diritto patrimoniale, è maggiore. Nella truffa, invece, poiché il privato danneggiato è stato causa del proprio danno, l'allarme sociale destato è minore e questo giustifica una pena più lieve[135]. Tuttavia, nella frode informatica non è la vittima ad effettuare la disposizione patrimoniale, ma lo stesso reo, seppur tramite il sistema in informatico. Il fondamento dell'equiparazione dipende piuttosto dall'assenza di conflitto sul "possesso" della *res*, trattandosi di un "aggiramento" patrimoniale. In ogni caso, come si vedrà nel prosieguo, questa aporia riguardante l'identico trattamento sanzionatorio è oggi attenuata dall'introduzione della nuova circostanza aggravante di cui al co. 2 per l'ipotesi in cui il fatto produca un trasferimento di denaro, di un valore monetario o di valuta virtuale.

Nell'ambito applicativo della norma in questione possono rientrare tutti quei casi in cui il reo manipola il sistema di *home banking* o similari per effettuare disposizioni patrimoniali non autorizzate dal soggetto passivo. Dunque, vi rientrano senz'altro gli attacchi *man-in-the middle*, ove il reo altera la destinazione dei bonifici, nonché il *pharming*, ove il soggetto manipola il computer della vittima cambiando i domini della lista dei preferiti al fine di penetrare nel sistema. Non solo, ma è punibile ai sensi della norma in questione anche la condotta di colui che si appropria delle chiavi del *wallet* e delle criptovalute ivi custodite, visto che per far ciò deve necessariamente manipolare il sistema informatico o comunque intervenire su di esso senza diritto.

Più problematico, invece, è proprio il caso del *phishing* classico. In questo, infatti, il contenuto del messaggio di posta elettronica, il *link* di indirizzamento alla pagina *web* non autentica e la struttura grafica di quest'ultima integrerebbero oggettivamente un artificio tale da creare nel destinatario una falsa rappresentazione della realtà, inducendolo in errore e generando un motivo per l'agire fondato su una falsa convinzione[136]. Gli utenti forniscono i propri dati personali relativi all'accesso ai servizi bancari o finanziari, indotti in errore tramite i suddetti artifici, ed a causa di ciò subiscono una diminuzione patrimoniale a causa del successivo utilizzo degli estremi delle loro carte di credito o delle credenziali di *home banking* da parte dell'imputato, che determina altresì l'ingiusto profitto per quest'ultimo o per terzi. Per una parte della giurisprudenza e della dottrina, dunque, in caso di *phishing classico* difetterebbe l'elemento costitutivo della frode informatica, ovvero l'alterazione del sistema

[135] SGUBBI F., voce *Patrimonio (reati),* cit., p. 341.
[136] FIANDACA G., MUSCO E., *Dir. pen.*, *PS*, vol. 2, VI ed., Bologna, 2014, p. 188.

informatico e si configurerebbe la diversa fattispecie di truffa comune[137].

Ciò posto, si evidenzia tuttavia che, stante la complessità del fenomeno criminoso in esame, è impossibile stabilire a priori se l'ultima fase dell'attività di "pesca fraudolenta" sia riconducibile alla fattispecie di frode informatica o di truffa comune: nel *pharming*, come esaminato, si realizza un'alterazione del funzionamento del sistema informatico al fine di indurre la vittima a fornire le proprie generalità e, quindi, si rientra sicuramente nelle condotte punite ex art. 640-*ter* c.p. quando ne consegue il doppio evento dell'ingiusto profitto con altrui danno[138], per cui non vi sarebbero gli elementi costitutivi della truffa.

Si può, però, provare ad effettuare una bipartizione: nei casi in cui il reo abbia fraudolentemente operato con *software* autoinstallanti sul sistema informatico, si configurerà il delitto di frode informatica, data l'avvenuta alterazione del funzionamento della macchina dell'utente, conseguente all'unilateralità aggressiva del fatto illecito. Diversamente, si configurerà la truffa comune nel caso in cui il reo proceda mediante l'invio di *e-mail* fasulle e/o *link* a siti clone, nei quali la vittima inserisce le proprie credenziali, poiché tale attività non si traduce in un'alterazione o in un intervento senza diritto sul sistema, ma vi è la cooperazione artificiosa della vittima, secondo lo schema tipico della truffa comune[139]. Tuttavia, questa bipartizione non è da tutti condivisa, in particolare quando in quest'ultimo caso sia il reo ad effettuare la disposizione patrimoniale sostituendosi al soggetto passivo[140]. Si osserva, infatti, che l'evento della disposizione patrimoniale è un requisito implicito del delitto di truffa, il quale rappresenta l'effetto dell'errore ed è il tramite causale del danno patrimoniale, espressivo della necessaria cooperazione da parte della vittima e, in tal senso, frutto della falsa rappresentazione della realtà. Si sostiene, quindi, che tale requisito costituisca un limite all'applicazione dell'art. 640 c.p. ai casi di *phishing attacks* in cui non vi sia stato alcun atto, negoziale o meno, commissivo o omissivo, realizzato dallo stesso soggetto ingannato e che abbia provocato gli eventi, di natura patrimoniale, di danno per il soggetto passivo e di profitto per il soggetto agente o per un terzo. Non si potrebbe quindi

---

[137] In giurisprudenza, infatti, è prevalsa la tesi della configurabilità della truffa: così Cass. pen., sez. VI, 4 ottobre 1999, n. 3065, Trib. Milano, Ufficio G.I.P., 7 novembre 2007, cit.; Trib. Milano, Ufficio G.I.P., 29 ottobre 2008, n. 8542, cit.; In dottrina v. anche CAJANI F., *Profili penali del phishing*, cit., p. 2296; PERRI P., *Lo smishing e il vishing*, cit., p. 267. Tale scelta però non è univoca, *a contrariis* v. anche Cass. pen., sez. V, 24 novembre 2003, n. 4576 e Cass. pen., sez. II, 24 febbraio 2011, n. 9891.

[138] CAJANI F., *La tutela penale dell'identità digitale alla luce delle novità introdotte dal d.l. 14 agosto 2013, n. 93 (convertito con modificazioni dalla l. 15 ottobre 2013, n. 119)*, in *Cass. pen.*, n. 3, 2014, p. 1094 ss., p. 1097. Sul fenomeno del *pharming* v. *supra*, cap. I, par. 6.

[139] BISORI L., *Le frodi informatiche*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (a cura di), *Trattato di diritto penale. Parte speciale*, X ed., Torino, 2011, 604 ss., 614; MINICUCCI, *Le frodi informatiche*, cit., p. 842.

[140] FLOR R., *Phishing, identity theft,* cit., p. 903.

ricadere sotto l'ambito applicativo di questa fattispecie ove il reo, dopo aver ottenuto i dati riservati tramite la falsa rappresentazione della realtà, abbia effettuato egli stesso l'accesso abusivo al sistema bancario dell'istituto di credito, eseguendo direttamente operazioni bancarie o finanziarie a proprio profitto[141]. In questo caso si configurerebbe, invece, la fattispecie di frode informatica, posto che l'aver eseguito disposizioni di pagamento accedendo al sistema di *home banking* della vittima sarebbe qualificabile come "*intervento senza diritto su dati, informazioni o programmi"*. Quest'ultima interpretazione appare senz'altro preferibile, posto che, come già evidenziato, ciò che differenzia la frode informatica dalla truffa comune è proprio la mancanza dell'atto di disposizione da parte della vittima quale conseguenza diretta dell'errore in cui sia stata indotta.

La frode informatica è aggravata: «*se ricorre una delle circostanze previste dal n. 1 del secondo comma dell'art. 640*[142]*»,* «*se il fatto è commesso con abuso della qualità di operatore del sistema*» e, a seguito del d.lgs. 8 novembre 2021, n. 184, «*se il fatto produce un trasferimento di denaro, di valore monetario o di valuta virtuale*». Inoltre, a seguito della novella introdotta dal d.l. 14 agosto 2013, n. 93, convertito con modificazioni dalla l. 15 ottobre 2013, n. 119, si ha un forte aggravamento di pena «*se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di una o più persone*». Anche in questo caso, come già evidenziato per l'art. 615-*ter* c.p. (v. *supra*, cap. II, par. 2) si ripropone il problema dell'individuazione di quali siano i soggetti che possiedono la qualifica di "operatore del sistema". Pure qui la dottrina si divide tra coloro che sostengono che si debba trattare dell'amministratore del sistema, o comunque di colui che ha il controllo delle diverse fasi del procedimento di elaborazione dei dati nonché l'opportunità di inserirsi nella memoria interna del sistema attraverso un canale di accesso privilegiato[143], e coloro che, invece, ritengono che possa essere anche il semplice addetto[144]. La giurisprudenza, invece, ha qualificato come operatore del sistema colui che in qualità di operatore, programmatore o analista, deve necessariamente avvalersi di un sistema informatico per le mansioni del suo ufficio[145].

Problemi del tutto peculiari presentano poi le due circostanze aggravanti speciali del

---

[141] *Ibid*., p. 906.

[142] Ovvero «*se il fatto è commesso a danno dello stato o di un altro ente pubblico o col pretesto di far esonerare taluno dal servizio militare*».

[143] PECORELLA C., *Il diritto penale dell'informatica*, cit., p. 123

[144] BORRUSO R., *La tutela dei documenti e dei dati*, in R. Borruso, G. Buonomo, G. Corasaniti, G. D'Aietti (a cura di), *Profili penali dell'informatica*, cit., p. 33.

[145] Così Cass. pen., sez. II, sentenza 10 novembre 2009, n. 44720, secondo cui «*per operatore del sistema deve intendersi, nella ratio della norma chiunque, nell'ambito del sistema informatico svolge una funzione dal cui abuso può derivare un'agevolazione nella perpetrazione del reato*».

fatto commesso con furto e indebito utilizzo dell'identità digitale, nonché del fatto che produce un trasferimento di denaro, valore monetario o valuta virtuale.

2.1 L'ipotesi aggravata dal *«furto o indebito utilizzo dell'identità digitale»*

Come sopra evidenziato, l'art. 9 d.l. n. 93/2013 ha introdotto al terzo comma dell'art. 640-*ter* c.p.[146] una nuova circostanza aggravante ad effetto speciale del delitto di frode informatica, con l'intenzione di fornire una maggiore tutela penale alle ipotesi di furto di identità digitale. Lo scopo dell'intervento normativo in questione è di incrementare la tutela dell'identità digitale, al fine di aumentare la fiducia dei cittadini nell'utilizzazione dei servizi *online* e porre un argine al fenomeno delle frodi realizzate mediante la tecnica del *phishing*[147].

Tale circostanza aggravante è stata introdotta in via autonoma dal legislatore italiano, anche se va evidenziato che l'art. 9 par. 5 della direttiva 2013/40/UE impone agli Stati membri di prevedere una circostanza aggravante per le interferenze illecite di dati e sistemi commesse abusando dei dati personali di un'altra persona allo scopo di guadagnare la fiducia di terzi, in tal modo arrecando un danno al legittimo titolare dell'identità digitale[148]. La circostanza aggravante in questione, però, a differenza di quanto indicato nella normativa UE, accede al reato di frode informatica, non alle fattispecie in materia di danneggiamento di dati e sistemi informatici. Tuttavia, non si ravvisa alcun contrasto col diritto UE, dato che lo stesso art. 9 della direttiva obbliga gli Stati membri ad introdurre una circostanza aggravante di tal genere «*purché tale circostanza non sia già contemplata da un altro reato punibile a norma del diritto nazionale*».

Inizialmente sono sorti dei dubbi in merito alla sua qualificazione quale circostanza aggravante. Infatti, se da un lato vi sono elementi che fanno propendere per la sua configurazione quale circostanza aggravante ad effetto speciale, ve ne sono altri che invece rendono plausibile l'inquadramento come fattispecie autonoma. In particolare, ci si riferisce al fatto che la frode informatica è una fattispecie che tutela il patrimonio, mentre il furto d'identità ha una connotazione più ampia, perché non si limita alle sole diminuzioni

---

[146] «*La pena è della reclusione da due a sei anni e della multa da euro 600 a euro 3.000 se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti*».

[147] PISTORELLI L., *Relazione Ufficio del Massimario Cassazione*, n. III/01/2013 del 22 agosto 2013, consultabile al sito www.penalecontemporaneo.it

[148] «*Gli Stati membri adottano le misure necessarie ad assicurare che, qualora i reati di cui agli articoli 4 e 5 siano commessi abusando dei dati personali di un'altra persona allo scopo di guadagnare la fiducia di terzi, in tal modo arrecando un danno al legittimo proprietario dell'identità, ciò possa, conformemente al diritto nazionale, essere considerato una circostanza aggravante, purché tale circostanza non sia già contemplata da un altro reato punibile a norma del diritto nazionale*».

patrimoniali che da esso possono essere causate, ma può essere realizzato per ledere l'onore o la reputazione del soggetto ed in generale il diritto all'identità personale.

Tuttavia, viene ora pacificamente ritenuto che si tratti di una circostanza aggravante[149]. Innanzitutto, si evidenzia che in sede di approvazione parlamentare del d.l. è stato precisato che la sostituzione dell'identità rappresenta un'aggravante del delitto di frode informatica[150]. Inoltre, ad ulteriore sostegno di questa tesi, vi è la revisione dell'ultimo comma dell'art. 640-*ter* c.p., ove in materia di procedibilità si stabilisce che «*il delitto è punibile a querela della persona offesa salvo che ricorra taluna delle circostanze di cui al secondo e terzo comma o un'altra circostanza aggravante*», Pertanto, essa viene esplicitamente qualificata come circostanza. Appare, dunque, evidente che la scelta del legislatore è stata quella di introdurre una vera e propria circostanza aggravante in virtù della particolare modalità di verificazione della frode informatica, che in quanto tale accede al reato senza modificarne gli aspetti essenziali, ma quale mero elemento specializzante.

Si può quindi pacificamente ritenere che si tratta di una circostanza aggravante speciale perché riguardante solo il delitto di cui all'art. 640-*ter* c.p.[151] e ad effetto speciale perché l'aumento di pena ivi previsto è superiore ad un terzo rispetto alla pena prevista per la fattispecie base[152].

Va poi precisato che l'uso indebito dei dati o dell'identità digitale non deve necessariamente risolversi in danno della vittima dell'illegittima diminuzione patrimoniale, ma, data la presenza della locuzione "in danno di uno o più soggetti", è evidente che il furto o l'indebito utilizzo d'identità digitale non devono essere necessariamente stati commessi ai danni della vittima finale della frode[153].

La circostanza aggravante in esame presenta all'interprete ben tre problematiche: la definizione di "utilizzo" indebito di una identità digitale altrui, il rapporto e la differenza tra il "furto" e l'"indebito utilizzo" di identità digitale e il rapporto tra l'"indebito utilizzo" e

---

[149] MINICUCCI G., *Le frodi informatiche*, cit., p. 839; MANTOVANI F., *Diritto penale, PS*, cit., p. 226.; MARGIOCCO M., *Frode informatica*, cit., p. 1110.

[150] Intervento Onorevole A. Gargano tenutasi innanzi alla Camera dei Deputati, seduta n. 93 del 9/10/13, in www.camera.it.

[151] MANTOVANI F., *Dir. pen.*, *PG*, cit., p. 402.

[152] «*Il decreto legge non istituisce dunque un'autonoma fattispecie penale relativa al c.d. furto dell'identità digitale, ma prevede che la sostituzione di tale identità possa rappresentare un'aggravante del delitto di frode informatica*» Cfr. Dossier del Servizio studi del Senato sull'A.S. n. 1079, ottobre 2013, n. 64, p. 103, disponibile *online* al sito http://www.senato.it/service/PDF/PDFServer/BGT/00739574.pdf

[153] BISORI L., *Frode informatica (art. 640-*ter *c.p.)*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (a cura di), *Trattato di diritto penale. Parte generale e speciale. Riforme 2008-2015*, Torino, 2015, p. 921 ss., p. 923.

l'ipotesi base di frode informatica[154]. Il legislatore, infatti, non ha dato alcuna definizione di "identità digitale", scelta molto discutibile, perché oltre a creare difficoltà agli operatori del diritto pone anche seri problemi di legittimità costituzionale. La dottrina ha cercato quindi di individuare i confini dell'identità digitale ricercando definizioni espresse in sede extra-penale.

Il primo riferimento è contenuto nell'art. 1, co. 1, lett. e), del d.lgs. 82 del 2005, in cui è stato chiarito che per "identificazione informatica" si deve intendere la «*validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne consentono l'individuazione nei sistemi informativi, effettuata attraverso opportune tecnologie anche al fine di garantire la sicurezza dell'accesso»*. Si è tuttavia sin da subito rilevato che questa descrizione non può prestarsi a un'applicazione generalizzata, alla luce del fatto che l'art. 2, co. 1, dello stesso decreto, circoscrive la portata applicativa di questo testo normativo al solo fine di assicurare «*la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale».*

La disposizione in questione, del resto, è stata in seguito abrogata dall' art. 1, co.1, lett. h), d.lgs. 179 del 2016, che ha inserito all'art. 1, co. 1, del d.lgs. 82 del 2005, c.d. codice dell'amministrazione digitale, la lett. u *quater*), che espressamente definisce l'identità digitale come: «*la rappresentazione informatica della corrispondenza tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale secondo le modalità fissate nel decreto attuativo dell'articolo 64»*. Tuttavia, anche in questo caso si deve rilevare come le definizioni fornite dal Codice dell'Amministrazione Digitale siano espressamente valide ai soli fini del codice stesso[155].

I tentativi di trovare una definizione per tale nozione in sede extra-penale, quindi, si scontrano tutti col fatto che le diverse descrizioni sono state create *ad hoc* per i provvedimenti nei quali sono inserite e non sempre riescono a cogliere appieno la *ratio* sottesa all'introduzione dell'aggravante in esame nel sistema penale, specie se l'identità digitale è intesa come processo di identificazione informatica, perché in questo caso la nozione è limitata al momento della validazione in un sistema di un insieme di dati al fine di individuare all'interno di esso un soggetto utente di determinati servizi[156]. Tant'è che è stato

[154] MALGIERI G., *La nuova fattispecie di "indebito utilizzo d'identità digitale": un problema interpretativo,* in *Dir. pen. cont.- Riv. trim.,* n. 2, 2015, p. 143 ss., p. 144.
[155] Così come riportato nell'art. 1 del d.lgs. n. 82/2005 cit.
[156] Altre definizioni infatti sono: la prima quella introdotta ai soli fini della creazione e sviluppo del Sistema Pubblico per la gestione delle Identità Digitali di cittadini ed imprese, ove il decreto della Presidenza del Consiglio dei Ministri del 24 ottobre 2014 all'art. 1 c. 1 lett. o) definisce l'identità digitale come la «*rappresentazione informatica della corrispondenza biunivoca tra un utente e i suoi attributi identificativi,*

ipotizzato che nella costruzione di questa norma il legislatore volesse riferirsi alle credenziali di uso di un sito *web*[157]. In tal caso è facile intuire che l'"indebito utilizzo" dell'identità digitale finirebbe per coincidere con la violazione delle misure di sicurezza per l'accesso al sistema o per l'acquisizione di dati e informazioni[158]. Quest'ultima tesi è stata recentemente accolta anche dalla Cassazione, la quale ha escluso che la nozione di identità digitale di cui alla circostanza aggravante in questione presupponga una procedura di validazione adottata dalla pubblica amministrazione ed ha, invece, ritenuto che essa si riferisca anche a credenziali di accesso a sistemi informatici gestiti da privati, ad esempio il sistema di *home banking*[159].

Nel costruire quest'aggravante, poi, il legislatore non ha specificato in che cosa consista la condotta né del furto d'identità né del suo indebito utilizzo[160]. Peraltro, si evidenzia l'utilizzo improprio del termine "furto" riferito ad un'entità immateriale quale l'identità digitale, insuscettibile di appropriazione o di possesso. Un significativo aiuto su che cosa debba intendersi per "furto d'identità digitale" arriva però proprio dal legislatore stesso. In sede parlamentare[161] è stato infatti asserito che si debba fare riferimento all'art. 30-*bis* del d.l. 13 agosto 2010, n. 141[162]. Tuttavia, ove si ritenesse che il furto d'identità coincida con l'impersonificazione risulterebbe complesso stabilire l'ambito applicativo dell'indebito utilizzo dell'identità digitale, perché anche colui che fa utilizzo di un'identità per diversi fini rispetto a quelli per cui era stato autorizzato apparentemente impersonifica un altro soggetto[163].

Problematiche persino maggiori presenta la locuzione "indebito utilizzo". Nessun

---

verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale secondo le modalità di cui al presente decreto e dei suoi regolamenti attuativi», anche se in questo caso sembrerebbe far riferimento più ad una metodologia che consente l'identificazione informatica, piuttosto che ad un vero e proprio concetto di identità digitale; la seconda è contenuta nell'art. 3 il Reg. eIDAS, il quale però non fa riferimento al concetto di identità digitale, ma all'"identificazione elettronica" ed ai "dati di identificazione personale".

[157] *«In attesa delle prime applicazioni della norma in questione, si osserva che quanto al concetto di identità digitale, con ogni probabilità il legislatore ha inteso riferirsi alle credenziali di uso di un sito web»*, così MARGIOCCO M., *Frode informatica*, cit., p. 1110.

[158] così FLOR R., *La legge penale nello spazio*, cit., p. 171.

[159] Cass. pen., sez. II, sentenza 20 settembre 2022, n. 40862.

[160] MALGIERI G., *La nuova fattispecie*, cit., p. 144.

[161] Dossier del Servizio studi del Senato sull'A.S. n. 1079, cit., p. 102.

[162] «*a) l'impersonificazione totale: occultamento totale della propria identità mediante l'utilizzo indebito di dati relativi all'identità e al reddito di un altro soggetto. L'impersonificazione può riguardare l'utilizzo indebito di dati riferibili sia ad un soggetto in vita sia ad un soggetto deceduto; b) l'impersonificazione parziale: occultamento parziale della propria identità mediante l'impiego, in forma combinata, di dati relativi alla propria persona e l'utilizzo indebito di dati relativi ad un altro soggetto, nell'ambito di quelli di cui alla lettera a)*»

[163] *«Inoltre, ci si domanda come coniugare tale fattispecie* (N.d.R. L'indebito utilizzo) *con quella di "furto di identità": due condotte apparentemente eterogenee eppur legate da un medesimo giudizio di disvalore nell'aggravante in esame»* MALGIERI G., *La nuova fattispecie*, cit., p. 144.

aiuto per la comprensione della portata di questa condotta viene dai lavori parlamentari: anzi, vi è addirittura una discrasia normativa tra il *nomen iuris* dell'aggravante in questione, indicato nella rubrica dell'art. 9 del d.l. n. 93/2013, e quanto previsto dal testo della norma, proprio perché frutto di una modifica in sede di conversione. Per superare l'*impasse*, però, secondo la dottrina l'unico modo per descrivere l'indebito utilizzo e capire il suo rapporto col furto d'identità digitale è proprio far riferimento alla rubrica dell'articolo: «*sostituzione dell'identità digitale*». L'effetto delle due condotte sarebbe quindi identico, ma le modalità di esecuzione sarebbero differenti, perché nell'indebito utilizzo il possesso dei dati è lecito, ed è solo un determinato utilizzo non concordato che va a integrare la violazione, mentre nel furto di dati la violazione del consenso vi è già nel momento della ricezione dei dati[164]. Si può, quindi, ritenere che l'indebito utilizzo dell'identità digitale consista nella sostituzione tramite le tecnologie informatiche di un'altrui persona, ma i dati siano già legittimamente posseduti dall'autore per altri scopi, dunque nell'impiego non autorizzato dei dati in questione.

Le soluzioni individuate, tuttavia, non sono pienamente soddisfacenti. In particolare, il problema che si pone è se l'uso indebito dell'identità digitale possa configurarsi in qualsiasi momento del processo fraudolento oppure tale condotta sia riferita unicamente al momento dell'autenticazione. Un esempio può chiarire meglio: se il criminale informatico effettua un attacco informatico del tipo *man-in-the-middle*, nel quale, previa installazione di un *malware*, si limita ad intercettare i bonifici effettuati dalla vittima cambiando a suo favore l'IBAN del destinatario, tecnicamente non "utilizza indebitamente" le credenziali della vittima, poiché è quest'ultima che autonomamente effettua il *login*. Se, dunque, l'"indebito utilizzo" delle credenziali deve necessariamente avere come riferimento il momento dell'autenticazione, come peraltro sembrerebbe essere l'intenzione del legislatore, in questo caso non potrebbe ritenersi integrata l'aggravante di cui al co. 3 dell'art. 640-*ter* c.p. Tuttavia, il criminale riesce a ricevere i bonifici proprio facendo un utilizzo indebito dell'identità digitale della vittima e si finge operatore del sistema inoltrando le finte ricevute di ritorno dell'operazione. Questo aspetto, dunque, meriterebbe maggiore considerazione ai fini dell'applicabilità della circostanza aggravante in questione.

Infine, va ricordato che il "furto o indebito utilizzo di identità digitale" è concepito dal nuovo co. 3 art. 640-*ter* c.p. come un'aggravante della frode informatica, per cui restano fuori dall'ambito applicativo della circostanza aggravante in questione gli schemi

[164] *Ibid*., p. 151.

tradizionali di truffe *online*, ove il reo assume un'identità fittizia allo scopo di carpire la fiducia della vittima.

2.2. La nuova circostanza aggravante del fatto che «produce un trasferimento di denaro, di valore monetario o di valuta virtuale»

Con il d.lgs. 8 novembre 2021, n. 184, di attuazione della direttiva 2019/713/UE, il legislatore è poi intervenuto anche sulla fattispecie di frode informatica, inserendo una nuova circostanza aggravante «*se il fatto produce un trasferimento di denaro, di valore monetario o di valuta virtuale*».

Tale circostanza aggravante è stata introdotta perché l'art. 6 della citata direttiva imponeva l'adozione di misure necessarie a sanzionare l'atto di effettuare o indurre un trasferimento di denaro, di valore monetario o di valuta virtuale, arrecando illecitamente a terzi una perdita patrimoniale allo scopo di procurare un ingiusto profitto all'autore del reato o a una terza parte, se commesso intenzionalmente ostacolando, senza diritto, il funzionamento di un sistema di informazione o interferendo con esso, oppure introducendo, alterando, cancellando, trasmettendo o sopprimendo senza diritto dati informatici. Si evidenzia che già la decisione quadro 2001/413/GAI del Consiglio, oggi sostituita dalla sopra menzionata direttiva, all'art. 3 prevedeva l'adozione da parte degli Stati membri delle stesse identiche misure, con l'unica differenza dell'assenza del riferimento alla valuta virtuale. Tuttavia, in occasione del recepimento di tale decisione quadro il nostro legislatore non aveva sentito la necessità di modificare in alcun modo la fattispecie di frode informatica.

Diversamente, in occasione del recepimento della menzionata direttiva, il nostro legislatore ha sì sottolineato che le condotte previste all'art. 6 della direttiva già rientravano nell'ambito applicativo dell'art. 640-*ter* c.p., ma ha comunque deciso di introdurre tale nuova circostanza aggravante allo scopo di «*riparametrare a quello dell'articolo 493-ter c.p. il regime sanzionatorio di tali condotte*»[165].

Si osserva, però, che i margini applicativi di quest'ultima circostanza aggravante finiscono per coincidere con quelli della fattispecie base, poiché la frode informatica è un reato di evento, che richiede si realizzi il danno per la vittima, danno che, come sopra evidenziato, ha necessariamente connotazione patrimoniale[166]. Poiché, dunque, ai fini della configurabilità della frode informatica non si può prescindere dalla concreta dimostrazione dell'avvenuto spostamento economico dalla vittima al reo, il "trasferimento di denaro o

[165] V. la relazione illustrativa al d.lgs. 184/2021, disponibile *online* al sito «https://www.camera.it».
[166] PICA G., *Diritto penale delle tecnologie informatiche*, cit., p. 148 ss.

valore monetario o valuta virtuale" è già elemento costitutivo del reato. Pertanto, tale circostanza aggravante troverà applicazione alla totalità delle frodi informatiche. La frode informatica aggravata finisce così per divenire realisticamente l'ipotesi usuale di reato.

È infatti difficile anche solo immaginare una frode informatica che non abbia ad oggetto denaro o comunque un valore monetario. Dunque, più che inserire una nuova circostanza aggravante del genere sarebbe stato più opportuno limitarsi ad aumentare la pena prevista per l'ipotesi base della frode informatica.

Inoltre, la circostanza aggravante in questione fa specifico riferimento alla "valuta virtuale", contrapponendola al "valore monetario", senza tener conto che l'art. 2 lett. d) della stessa direttiva 2019/713/UE definisce la valuta virtuale come mezzo di scambio. Per cui, anche se non può essere classificata come moneta, ha comunque un suo valore economico. Peraltro, la stessa direttiva evidenzia che il suo ambito di applicazione dovrebbe essere limitato alle monete virtuali soltanto nella misura in cui possono essere comunemente utilizzate per effettuare pagamenti[167]. Dunque, sembra circoscrivere la tutela penale alla sola valuta che abbia una certa diffusione e caratteristiche tali da essere accettata da persone fisiche o giuridiche come mezzo di scambio. Pertanto, a maggior ragione non si comprende il motivo della contrapposizione tra i due concetti. Sia il valore monetario che la valuta virtuale, infatti, hanno un valore economico. La contrapposizione, però, è propria anche della stessa direttiva, che all'art. 6 espressamente distingue il "valore monetario" dalla "valuta virtuale", per cui la medesima critica va mossa anche al legislatore europeo. Peraltro, in epoca recente sono stati molti gli strumenti di pagamento diversi dai contanti adottati e dopo poco divenuti obsoleti, basti pensare agli *eurochèque*. Sarebbe stato, dunque, meglio prevedere una formula generica ed onnicomprensiva, in grado di adattarsi alla rapida evoluzione degli strumenti di pagamento.

3. L'indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti *ex* art. 493-*ter* c.p.

Concetto diverso rispetto a quello di frode informatica è quello di abuso e falsificazione di strumenti di pagamento diversi dai contanti. Tuttavia, va sin da subito sottolineato che la distinzione tra i due concetti non è così netta come potrebbe a prima vista sembrare: già in passato vi era chi aveva evidenziato che le carte di credito a microprocessore, che registrano nel *chip* ivi inserito tutti i movimenti di denaro effettuati,

[167] V. Considerando n. 10 della direttiva 2019/713/UE.

difficilmente possono distinguersi dal sistema informatico[168]. Inoltre, già prima della diffusione dei sistemi di pagamento immateriali, si era rilevato che la maggior parte degli abusi relativi alle carte di credito comporta un'alterazione in qualsiasi modo su dati, informazioni o programmi contenuti in un sistema informatico o telematico, che se procurano un ingiusto profitto con altrui danno rientrano nell'ambito applicativo della frode informatica[169]. Pertanto, come si esaminerà meglio nel prosieguo, l'individuazione dei rapporti tra le fattispecie menzionate è estremamente controversa.

Neppure il legislatore europeo è riuscito a distinguere in modo chiaro la frode informatica dalla falsificazione e indebito utilizzo di strumenti di pagamento diversi dai contanti, in particolare i nuovi strumenti immateriali, quali ad esempio le *App* di *home banking* per *smartphone*. Ciò, come si esaminerà in seguito, ha comportato l'adozione di soluzioni molto diverse tra loro da parte dei legislatori dei singoli Stati membri. Tant'è che in altri ordinamenti europei l'indebito utilizzo di strumenti di pagamento diversi dai contanti viene sanzionato quale frode informatica (v. Infra, cap. V, par. 5).

Nell'ordinamento italiano, però, vi è una netta distinzione tra fattispecie che sanzionano la falsificazione e/o l'indebito utilizzo di strumenti di pagamento diversi dai contanti e la frode informatica, differenza che si riflette anche con riferimento alle pene previste.

Il nostro legislatore introdusse per la prima volta una fattispecie in materia con l'art. 12 del d.l. 3 maggio 1991, n. 143, convertito poi con modificazioni dalla l. 5 luglio 1991, n. 197, intitolato "provvedimenti urgenti per limitare l'uso del contante e dei titoli al portatore nelle transazioni e prevenire l'utilizzazione del sistema finanziario a scopo di riciclaggio". Essa fu introdotta per via la difficoltà di ricondurre nell'ambito applicativo degli artifizi e raggiri della truffa il semplice utilizzo della carta[170] Tale fattispecie prevedeva tre ipotesi di reato concettualmente distinte, anche se punite con la medesima pena[171]. Inizialmente la norma in questione era collocata nella normativa antiriciclaggio, collocazione che veniva ritenuta poco funzionale, data la dubbia connessione tra gli abusi descritti nella norma e la funzione di prevenzione del riciclaggio propria della normativa del 1991[172].

---

[168] MILITELLO V., *La tutela penale dei nuovi strumenti di pagamento: il caso del «sistema eurochecque»*, in *Foro it*., 1992, vol. 115, p. 617 ss., p. 620.
[169] *Ibid*., p. 620.
[170] PECORELLA C., *Il nuovo diritto penale delle "carte di pagamento"*, in *Riv. it. dir. proc. pen*., 1993, n. 1, p. 235 ss., p. 243.
[171] PICA G., *Diritto penale delle tecnologie informatiche*, cit., p. 163.
[172] PICA G., *Diritto penale delle tecnologie informatiche*, cit., p. 164. MILITELLO V., *La tutela penale dei nuovi strumenti di pagamento*, cit., p. 618, benché critico nei riguardi della collocazione della norma, evidenziava però che la stessa poteva trovare la sua *ratio* nel fatto che il presidiare penalmente i nuovi strumenti

In seguito, il menzionato art. 12 fu abrogato dal d.lgs. 21 novembre 2007, n. 231 ed il contenuto della norma fu trasferito senza modifiche nell'art. 55 co. 5 dello stesso d.lgs. 231/2007, che dava attuazione alla direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo. Nonostante la differente collocazione, la norma rimase comunque situata nell'ambito della normativa antiriciclaggio.

Con l'art. 4, co. 1 lett. a) del d.lgs. 1 marzo 2018, n. 21, di attuazione del principio della c.d. riserva di codice, la disciplina penale delle carte di pagamento è stata finalmente inserita nel codice penale quale nuovo art. 493-*ter* c.p., nel capo delle fattispecie volte a contrastare le falsità in atti. Nonostante la collocazione della norma sia senz'altro più appropriata della precedente, vi è chi ha evidenziato che in realtà appaiono correttamente inserite unicamente le ipotesi di falsificazione o alterazione delle carte di pagamento, nonché il possesso e/o indebito utilizzo di carte falsificate o alterate, visto che le fattispecie di indebita utilizzazione, possesso, cessione o acquisizione di carte di pagamento nulla hanno in comune con la tutela della fede pubblica[173]. In tale occasione il legislatore si è limitato a trasferire la fattispecie già prevista all'art. 55 cit. senza apportarvi sostanziali modifiche.

Infine, l'art. 493-*ter* c.p. è stato oggetto di modifiche da parte del d.lgs. 184 del 2021, a partire dalla sua rubrica, che ora si intitola «*indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti*». Nonostante tale ultima modifica, si può affermare che la tutela penale delle carte di pagamento è rimasta formalmente identica sin dal momento della sua introduzione.

La norma sanziona l'utilizzazione indebita, da parte di soggetto diverso dal titolare, di carte di credito o di pagamento o di qualsiasi altro documento analogo che abiliti al pagamento del denaro contante, nonché ogni altro strumento di pagamento diverso dai contanti, la falsificazione o alterazione degli stessi, nonché il loro possesso, cessione o acquisizione. La norma in questione, dunque, sanziona sia l'indebito uso delle carte in questione, sia gli atti preparatori e prodromici all'uso, quali la falsificazione e il possesso. Si ha utilizzo quando dall'uso della carta si trae quell'utilità che essa, conformemente alla funzione che le è propria, è in grado di fornire[174]. L'utilizzazione deve avvenire "indebitamente", locuzione che va ricollegata al fatto che l'autore del fatto non è il titolare

di pagamento, oltre a tutelare specificamente gli interessi a questi collegati risulta funzionale all'obiettivo della lotta contro il riciclaggio.

[173] GALANTE A., *La tutela penale delle carte di pagamento*, in *Cybercrime*, cit., p. 285 ss., p. 287.

[174] PECORELLA C., *Il nuovo diritto penale delle "carte di pagamento"*, cit., p. 262.

della carta[175]. Dunque, deve ritenersi riconducibile al reato in esame ogni forma di utilizzo posto in essere da colui che non risulti titolare o legittimo possessore della carta o del documento[176]. Il reato in esame secondo la giurisprudenza è integrato anche nel caso in cui il terzo che utilizzi la carta sia stato autorizzato dal titolare, in quanto la legittimazione all'impiego del documento è contrattualmente conferita dall'istituto emittente al solo intestatario, il cui consenso all'eventuale utilizzazione da parte di un terzo sarebbe del tutto irrilevante[177].

La falsificazione consiste nella contraffazione, ossia nella formazione di una carta di pagamento simile a quella autentica, mentre l'alterazione del documento si ha con qualsiasi indicazione diversa da quelle apposte originariamente sulla carta dal soggetto che l'ha rilasciata[178]. L'alterazione può riguardare sia la modificazione dell'intestazione e dei dati sovraimpressi sulla carta, sia l'alterazione dei dati inseriti nella banda magnetica o nel chip[179]. Peculiarità è che in questo caso la norma non subordina la punibilità all'uso del documento falso, ma la anticipa al momento della contraffazione o alterazione del documento[180].

Per quanto riguarda l'ipotesi del possesso, la sua illiceità presuppone la provenienza illecita della carta[181]. Il possesso di tali strumenti è punito sin dall'introduzione della norma e consente una notevole semplificazione probatoria nei casi di clonazione, poiché il mero possesso della carta clonata consente di punire il soggetto indipendentemente dalla necessità di provare che lo stesso abbia preso parte alla falsificazione[182]. A tal proposito, si evidenzia che la sua incriminazione era stata richiesta dall'art. 2 della menzionata decisione quadro 2001/413/GAI ed è oggi imposta dall'art. 4 della direttiva 2019/713/UE. Oltre al possesso costituiscono reato sia l'acquisizione che la cessione dei documenti menzionati, che indicano qualsiasi tipo di trasferimento, gratuito od oneroso, della carta di credito illecitamente ottenuta, ovvero illecitamente modificata[183]. La norma, dunque, sanziona anche ipotesi che

[175] PICA G., *Diritto penale delle tecnologie informatiche*, cit., p. 164.
[176] PARODI C., *Commercio elettronico e tutela penale dei mezzi di pagamento*, in *Dir. pen. proc*., 2001, n. 1, p. 103 ss., p. 105.
[177] Cass. pen., sez. II, sentenza 17 settembre 2020, n. 26807; Cass. pen., sez. II, sentenza 22 febbraio 2019, n. 17453.
[178] PICA G., *Diritto penale delle tecnologie informatiche*, cit., p. 164.
[179] CORRADINO M., *La tutela penale del sistema dei pagamenti nell'abuso di carta di credito*, in *Banca, borsa, tit. cred*., 2001, n. 1, p. 121 ss., p. 126.
[180] PICA G., *Diritto penale delle tecnologie informatiche*, cit., p. 165.
[181] *Ibid*., p. 164.
[182] GALANTE A., *La tutela penale delle carte di pagamento*, cit., p. 289.
[183] PICA G., *Diritto penale delle tecnologie informatiche*, cit., p. 165.

possono non aver nulla a che fare con manipolazioni informatiche, né coi reati informatici in senso stretto[184].

L'art. 493-*ter* c.p. è una disposizione a più norme, perché prevede autonome incriminazioni di diverse forme di abuso delle carte di credito[185]. Poiché trattasi di ipotesi diverse e tra loro eterogenee sotto l'aspetto fenomenico, nel caso in cui il soggetto falsifichi una carta e successivamente la utilizzi indebitamente si configura necessariamente un concorso di reati[186].

Si ritiene che il bene giuridico tutelato dalla norma in questione non sia solo il patrimonio del titolare della carta di credito, ma anche la funzionalità, stabilità e credibilità nel sistema dei pagamenti[187]. Trattasi, pertanto, di reato plurioffensivo[188]. Per questo motivo, la giurisprudenza non solo esclude l'applicabilità alla norma in questione della scriminante del consenso dell'avente diritto, trattandosi di fattispecie a tutela di un interesse pubblicistico[189], ma anche l'applicabilità dell'attenuante del danno patrimoniale di speciale tenuità. In quest'ultimo caso si è evidenziato che il reato in questione, in quanto inteso a salvaguardare, oltre che la fede pubblica, l'interesse pubblico fondamentale a che il sistema elettronico di pagamento sia sempre utilizzato in modo corretto, è incompatibile con la circostanza attenuante in questione, in quanto l'evento dannoso o pericoloso non può dirsi connotato da ridotto grado di offensività e disvalore sociale solo perché il danno patrimoniale è tenue[190].

---

[184] PICOTTI L., voce *Reati informatici*, cit., p. 8.

[185] CORRADINO M., *La tutela penale del sistema dei pagamenti nell'abuso di carta di credito*, cit., p. 121.

[186] Tesi accolta dalle Sezioni Unite, v. Cass. pen., sez. un., sentenza 28 marzo 2001, n. 22902. In senso conforme Cass. pen., sez. II, sentenza 15 novembre 2011, n. 41696 e Cass. pen. sez. II, sentenza 13 febbraio 2014, n. 7019.

[187] CORRADINO M., *La tutela penale del sistema dei pagamenti nell'abuso di carta di credito*, cit., p. 135. In tal senso anche Corte cost., sentenza 19 luglio 2000, n. 302, secondo cui «*apprestando una più adeguata tutela penale alle carte di credito e ai documenti equiparati - in precedenza non garantita dalle norme incriminatrici comuni in tema di delitti contro il patrimonio - il legislatore del 1991 ha inteso incentivare, cioè, il ricorso a strumenti alternativi al denaro contante e che consentono l'identificazione dell'autore delle transazioni, quale mezzo di prevenzione del riciclaggio. Se, dunque, la norma incriminatrice mira, in positivo, a presidiare il regolare e sicuro svolgimento dell'attività finanziaria attraverso mezzi sostitutivi del contante, ormai largamente penetrati nel tessuto economico, è giocoforza ritenere che le condotte da essa represse assumano - come del resto riconosciuto anche dalla giurisprudenza di legittimità in sede di analisi dei rapporti tra la fattispecie criminosa in questione ed i reati di truffa e di ricettazione - una dimensione lesiva che comunque trascende il mero patrimonio individuale, per estendersi, in modo più o meno diretto, a valori riconducibili agli ambiti categoriali dell'ordine pubblico o economico, che dir si voglia, e della fede pubblica*».

[188] Cass. pen., sez. II, sentenza 8 aprile 2011, n. 15834; Cass. pen., sez. II, sentenza 25 settembre 2019, n. 47135.

[189] Cass. pen., sez. II, sentenza 16 febbraio 2021, n. 18609.

[190] Cass. pen., sez. II, sentenza 18 settembre 2020, n. 27432; Cass. pen., sez. II, sentenza 18 aprile 2019, n. 34466; Cass. pen., sez. II, sentenza 15 novembre 2012, n. 45902; Cass. pen., sez. IV, sentenza 13 dicembre 2019, n. 2319; Cass. pen., sez. II, sentenza 18 luglio 2017, n. 40875; Cass. pen., sez. VII, ordinanza 12 dicembre 2016, n. 2835.

Per quanto riguarda il soggetto attivo, la norma prevede espressamente che non deve trattarsi del titolare della carta[191]. Trattasi comunque di reato comune, realizzabile da chiunque, col solo limite del soggetto titolare della carta stessa[192].

L'oggetto materiale della tutela è comune a tutte e tre le fattispecie ed è costituito dalle carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi. Per quanto riguarda il concetto di carte di pagamento, sin dall'introduzione della norma si ritenne che non indicasse unicamente i mezzi di pagamento veri e propri alternativi al denaro contante, ma anche le carte che consentono di ottenere dall'emittente una somma di denaro, come ad esempio la tessera Bancomat, nonché quelle che pur non essendo mezzi di pagamento intervengono a rafforzare la fiducia nel pagamento compiuto con mezzi alternativi al denaro contante, quali la carta-assegni[193]. La categoria delle carte di pagamento, dunque, ricomprende al suo interno non solo le carte di credito, ma anche quelle di debito, nonché le carte prepagate e quelle a spendibilità limitata[194].

Progressivamente dalla tutela della carta intesa in senso materiale, gli interpreti si erano spostati verso la tutela delle funzioni di pagamento cui la carta abilita, in particolare l'utilizzo virtuale dei codici identificativi ed autorizzativi della carta[195]. Quest'operazione ermeneutica, però, presentava diversi limiti, in particolare con riferimento al divieto di analogia in *malam partem*.

A seguito del d.lgs. 184 del 2021, l'oggetto di tutti i reati ivi previsti è stato ampliato sino a ricomprendere tutti gli strumenti di pagamenti diversi dai contanti, non solo le carte di credito. Infatti, la precedente fattispecie, nonostante l'interpretazione estremamente lata ad essa fornita, era imperniata sul concetto di "documento", che richiedeva la fisicità dello stesso. Per questo motivo era dibattuto se la tutela apprestata dalla norma potesse essere estesa anche ai dati identificativi delle carte di credito[196]. Tale modifica legislativa ha adeguato la fattispecie ai mutamenti tecnologici. Grazie all'ampia formulazione adottata tramite l'inserimento del sintagma espansivo «*o comunque ogni altro strumento di pagamento diverso dai contanti*», il problema sopra esposto può oggi dirsi superato. Tale locuzione è indice del passaggio dalla tutela della carta di credito in senso materiale, alla

[191] PECORELLA C., *Il nuovo diritto penale delle "carte di pagamento"*, cit., p. 260.
[192] GALANTE A., *La tutela penale delle carte di pagamento*, cit., p. 295.
[193] PECORELLA C., *Il nuovo diritto penale delle "carte di pagamento"*, cit., p. 236.
[194] GALANTE A., *La tutela penale delle carte di pagamento*, cit., p. 290.
[195] *Ibid*., p. 289.
[196] *Ibid*.

tutela delle funzioni di pagamento cui il supporto abilita, ora svolte ad esempio anche da uno *smartphone* o da uno *smartwatch.* In questo modo, a differenza di altri legislatori europei (v. *infra* cap. V, par. 5) il nostro ha scelto di dare attuazione con una sola norma sia all'art. 4 (Reati connessi all'utilizzazione fraudolenta di strumenti di pagamento materiali diversi dai contanti) sia all'art. 5 (Reati connessi all'utilizzazione fraudolenta di strumenti di pagamento immateriali diversi dai contanti) della direttiva 2019/713/UE.

Il nostro legislatore all'art. 1 del d.lgs. 184 del 2021 ha poi fornito le definizioni di "strumento di pagamento diverso dai contanti", "dispositivo, oggetto o record protetto", "mezzo di scambio digitale" e "valuta virtuale". Tali definizioni sono identiche a quelle contenute nella Direttiva, inserite dal legislatore europeo proprio al fine di garantire uniformità nella sua applicazione e facilitare la cooperazione tra le autorità competenti. In particolare, la definizione di "strumento di pagamento" specifica che esso può essere immateriale o materiale. Dunque, si può affermare senza ombra di dubbio che oggetto del reato di cui all'art. 493-*ter* c.p. siano anche le *App* per *smartphone* e i programmi *software* di *home banking* diffusi dalle Banche per effettuare pagamenti *online*. Poiché non è specificato che lo strumento in questione debba essere necessariamente controllato da una banca centrale o da un ente pubblico, si ritiene che oggetto di tutela siano anche piattaforme di *mobile payment*, quali ad esempio *Satispay* o *PayPal*, che consentono di inviare a e ricevere fondi da altri utenti della stessa *App* senza utilizzare i circuiti di carte di credito e debito tradizionali. Per il resto l'art. 493-*ter* c.p. è rimasto invariato[197].

Per quanto riguarda l'elemento soggettivo, tutte le fattispecie di cui all'art. 493-*ter* c.p. sono caratterizzate dall'indicazione della finalità di profitto, per sé o per altri. Trattasi, pertanto, di reati puniti a titolo di dolo specifico[198].

L'ampiamento dell'oggetto delle fattispecie di cui all'art. 493-*ter* c.p. pone qualche difficoltà con riferimento ai rapporti tra quest'ultimo reato e la fattispecie di frode informatica. Infatti, in materia di utilizzo di carte di credito clonate era già sorto un contrasto giurisprudenziale circa la qualificazione giuridica del fatto[199]. Secondo un primo orientamento, la fattispecie applicabile sarebbe unicamente la frode informatica, in quanto l'elemento specializzante consisterebbe nell'utilizzazione "fraudolenta" del sistema

[197] BERTOLESI R., *Sub art. 493*-ter, in E. Dolcini, G.L. Gatta (a cura di), *Codice penale commentato,* V ed., Milano, 2021, §6; CORRADINO M., *La tutela penale del sistema dei pagamenti nell'abuso di carta di credito*, in *Banca, borsa, tit. cred.*, 2001, n. 1, p. 121 ss., p. 121.
[198] PARODI C., *Commercio elettronico e tutela penale dei mezzi di pagamento*, cit., p. 104.
[199] Contrasto giurisprudenziale rilevato anche dalla Cass. pen., sez. II, 14 febbraio 2017, n. 8913, la quale tuttavia non si è pronunciata sul punto, limitandosi ad annullare senza rinvio la sentenza impugnata per intervenuta prescrizione.

informatico, che assorbirebbe la generica indebita utilizzazione di una carta di credito[200]. Per un diverso orientamento, invece, integra il reato di indebita utilizzazione di carte di credito e non quello di frode informatica il prelievo di denaro contante presso lo sportello *bancomat* di una banca mediante l'abusivo utilizzo di supporti magnetici con dati clonati, perché non vi sarebbe né l'alterazione del sistema informatico o telematico, né l'abusivo intervento sui dati e quindi non sarebbero integrati gli elementi costitutivi della frode informatica[201]. Il quadro normativo è stato ora ulteriormente complicato, perché se prima della modifica legislativa si riteneva che l'uso di codici e numeri di carte di credito clonate per penetrare abusivamente nel sistema informatico bancario ed effettuare indebitamente operazioni integrasse la sola fattispecie di frode informatica e non l'indebita utilizzazione di carte di credito[202], ora non è più così pacifico. Infatti, in precedenza si riteneva che l'elemento specializzante dell'utilizzazione "fraudolenta" del sistema informatico, dunque la sua alterazione, costituisse presupposto "assorbente" rispetto alla generica indebita utilizzazione dei codici d'accesso. Tuttavia, gli strumenti di pagamento diversi dai contanti non possono essere falsificati se non attraverso l'alterazione di dati o programmi informatici, dato che si tratta di supporti immateriali. L'elemento dell'alterazione, dunque, perde il suo carattere di specialità e diventa così difficile individuare quale sia la norma prevalente.

Se, in definitiva, è da accogliere con favore il fatto che il nostro legislatore abbia scelto di attualizzare la norma in questione in modo da ricomprendervi i nuovi strumenti di pagamento, va però evidenziato che non si è minimamente preoccupato di disciplinare i rapporti tra l'art. 493-*ter* c.p. e la frode informatica. A ben guardare, però, neppure la stessa direttiva si è occupata di tracciare una netta demarcazione tra la falsificazione e l'indebito utilizzo degli strumenti di pagamento diversi dai contanti e la frode informatica. Infatti, all'art. 5 della direttiva ha dapprima previsto diverse misure obbligando gli stati membri a punire determinate condotte connesse all'utilizzazione fraudolenta di strumenti di pagamento immateriali diversi dai contanti, mentre il successivo art. 6 ha riguardato la "frode connessa

[200] In tal senso Cass. pen., sez. II, 15 aprile 2011, n. 17748, secondo cui «*integra il delitto di frode informatica, e non quello di indebita utilizzazione di carte di credito, colui che, servendosi di una carta di credito falsificata e di un codice di accesso fraudolentemente captato in precedenza, penetri abusivamente nel sistema informatico bancario ed effettui illecite operazioni di trasferimento fondi, tra cui quella di prelievo di contanti attraverso i servizi di cassa continua*»; in senso conforme anche Cass. pen., sez. II, 13 ottobre 2015, n. 50140, la quale in motivazione ritiene decisiva la sussistenza dell'elemento specializzante, costituito dall'utilizzo "fraudolento" del sistema informatico. Per la dottrina v. LAZZARI C., *Riciclaggio di carte di credito e truffa: concorso di reati o concorso di norme?*, in Cass. pen., 2001, n. 9, p. 2473.

[201] Così Cass. pen., sez. VI, 14 gennaio 2016, n. 1333.

[202] V. Cass. pen., sez. II, sentenza 21 luglio 2020, n. 21831; Cass. pen., Sez. II, Sentenza, 09/05/2017, n. 26229; Cass. pen., Sez. II, 13/10/2015, n. 50140; Cass. pen. sez. II, sentenza 15 aprile 2011, n. 17748.

ai sistemi di informazione". La stessa direttiva, poi, all'art. 9 prevede sanzioni diverse per i due articoli in questione. Dunque, a prima vista sembrerebbe aver distinto nettamente i due fatti. A ben guardare, però, la clonazione di un'*App* di *home banking*, ad esempio, costituisce sia contraffazione o falsificazione fraudolenta di uno strumento di pagamento immateriale diverso dai contanti (art. 5 direttiva), sia alterazione senza diritto di dati informatici per effettuare un trasferimento di un valore monetario (art. 6 direttiva). È evidente, dunque, che la costruzione delle norme in questione non tiene conto della concreta fenomenologia e non consente di distinguere chiaramente in cosa consista la falsificazione e/o l'indebito utilizzo di strumenti di pagamento diversi dai contanti e in cosa, invece, la frode informatica. Questa sovrapposizione non è priva di effetti, perché, come si è visto e come si vedrà anche nel prosieguo, non aiuta i legislatori nazionali nell'adozione di un sistema efficace e coerente per reprimere i fenomeni criminosi in questione.

4. Il microsistema normativo concernente i danneggiamenti informatici

A venire in rilievo non sono unicamente le frodi informatiche. Come si è esaminato, i sabotaggi informatici, che sempre più spesso coinvolgono non solo sistemi informatici di imprese private, ma anche appartenenti allo Stato o enti pubblici, costituiscono manifestazione criminosa piuttosto frequente.

Con l'art. 9 della citata l. 23 dicembre 1993 n. 547 fu inserita nel codice penale una fattispecie intitolata «*danneggiamento di sistemi informatici e telematici*», volta a reprimere le condotte di aggressione ai sistemi informatici nel loro complesso, dirette anche contro le componenti immateriali[203]. In questo modo, il nostro legislatore ha ovviato alla necessità di prevedere una specifica incriminazione per i fatti di danneggiamento che ricadono esclusivamente sul *software*, non assimilabile alla nozione di "cosa mobile"[204]. La norma in questione fu collocata immediatamente dopo l'art. 635 c.p., che disciplina il danneggiamento tradizionale, inquadramento che fu ritenuto corretto, dato che la norma offre tutela al bene informatico sotto il profilo patrimoniale[205]. L'art. 1 della l. n. 547 del 1993 ha poi esteso in termini generali la nozione di "violenza sulle cose" di cui all'art. 392 co. 3 c.p., specificando che «*si ha altresì, violenza sulle cose allorché un programma informatico viene alterato, modificato o cancellato in tutto o in parte ovvero viene impedito o turbato il funzionamento*

[203] PECORELLA C., *Il nuovo diritto penale delle "carte di pagamento"*, cit., p. 176.
[204] PICOTTI L. *voce Reati informatici*, cit., p. 18; PICA G., *Diritto penale delle tecnologie informatiche*, cit., p. 86; BERGHELLA F., BLAIOTTA R., *Diritto penale dell'informatica e beni giuridici*, cit., p. 2337.
[205] PICA G., *Diritto penale delle tecnologie informatiche*, cit., p. 87.

di un sistema informatico o telematico». Tale concetto, anche se affiancato a quello tradizionale di violenza sulle cose, in realtà si differenzia in modo significativo rispetto ad esso, perché la violenza in questo caso viene "rarefatta e idealizzata", slegata dal tradizionale effetto fisico-corporeo che fino a quel momento l'aveva caratterizzata[206]. Il legislatore del 1993 poi riformulò la fattispecie di attentato agli impianti di pubblica utilità di cui all'art. 420 c.p., estendendone l'ambito di operatività anche alle componenti immateriali di sistemi informatici di pubblica utilità ed in generale a tutto ciò che poteva essere funzionale al loro utilizzo[207].

Il sistema delle disposizioni concernenti i danneggiamenti informatici è poi stato notevolmente modificato ad opera della l. 18 marzo 2008, n. 48, di ratifica della Convenzione *Cybercrime*. Con tale intervento il legislatore ha dato attuazione alle sue disposizioni, distinguendo tra interferenza relativa ai dati e interferenza relativa ai sistemi. A differenza di altri legislatori europei, però, come si esaminerà meglio nel prosieguo, non si è limitato a prevedere queste due fattispecie incriminatrici, ma ha introdotto un vero e proprio "microsistema" normativo, composto da ben quattro fattispecie, differenziando la struttura dei reati e il trattamento sanzionatorio a seconda dell'oggetto di tutela[208]. Accanto all'art. 635-*bis* c.p., infatti, anch'esso modificato in tale occasione, sono state previste tre nuove ulteriori ipotesi delittuose, ovvero l'art. 635-*ter* c.p. (danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità), l'art. 635-*quater* c.p. (danneggiamento di sistemi informatici o telematici) e l'art. 635-*quinquies* c.p. (danneggiamento di sistemi informatici o telematici di pubblica utilità). Tale novella non ha incontrato il favore della dottrina, la quale ha evidenziato che la scelta di garantire ai sistemi "di pubblica utilità" una protezione rafforzata non richiedeva affatto una differenziazione in altrettanti distinti delitti, non prevista neppure dalle fonti sovranazionali[209]. Allo stesso tempo sono stati abrogati i co. 2 e 3 dell'art. 420 c.p., che disciplina per l'appunto il sabotaggio informatico, in modo da non creare sovrapposizioni con il nuovo art. 635-*quinquies* c.p. Tale scelta è stata oggetto di critiche non solo perché in questo modo il legislatore ha ritenuto gli attacchi, anche gravi, ai sistemi, dati, informazioni, programmi informatici pubblici o di pubblica utilità, come fatti inidonei a turbare l'ordine

[206] PICOTTI L. *voce Reati informatici*, cit., p. 16.
[207] Sul reato di sabotaggio ad impianti di pubblica utilità e sul problema della riconducibilità a titolo di danneggiamento degli atti di sabotaggio ad impianti di elaborazione dati prima della riforma v. PICOTTI L., *La rilevanza penale degli atti di "sabotaggio" ad impianti di elaborazione dati*, in *Dir. inf. inf*., 1986, n. 3, p. 969 ss., p. 972 ss.
[208] SALVADORI I., *Il "microsistema" normativo concernente i reati informatici*, cit., p. 206 s.
[209] PICOTTI L., *La ratifica della Convenzione Cybercrime*, cit., p. 715.

pubblico, ma anche, e soprattutto, perché in questo modo è venuto meno il riferimento alla tutela degli impianti informatici[210].

Per quanto riguarda il bene giuridico tutelato dalle fattispecie in questione, per un primo orientamento si tratta del patrimonio[211]. Si è però precisato che il valore economico del bene non va immaginato e commisurato unicamente al mero valore di mercato dell'apparato fisico danneggiato, poiché ciò che rileva maggiormente è il valore dei contenuti del sistema informatico, nonché la funzione che essi svolgono[212].

Altri evidenziano che dalla formulazione delle fattispecie emerge come il legislatore abbia voluto sanzionare un'ampia gamma di fatti non autorizzati che compromettono l'integrità, la disponibilità, l'autenticità e la regolare accessibilità di dati, programmi e sistemi informatici, per cui bene giuridico tutelato è l'integrità e disponibilità di dati e sistemi informatici[213].

Soggetto attivo di tutti i reati facenti parte di questo c.d. microsistema può essere chiunque, con la sola esclusione, nel caso degli artt. 635-*bis* e 635-*quater* c.p., del legittimo titolare dei dati, informazioni o programmi o del sistema, dato che in entrambi è presente l'inciso "altrui"[214]. Anche in questo caso si pone il problema di individuare la portata della nozione di "altruità", ovvero stabilire se la stessa vada interpretata rigidamente, intendendola come "di proprietà di altri" oppure se possa essere intesa in senso più ampio, comprensivo del danneggiamento compiuto dal proprietario della cosa in danno di chi esercita su di essa un diritto di godimento[215]. A tal proposito, è stato evidenziato che le nozioni di "proprietà" e "possesso" mal si adattano alla realtà immateriale di dati e sistemi informatici[216]. Si evidenzia, poi, che sono noti e frequenti i casi di danneggiamento da parte del proprietario del computer o del *software* concesso in uso ad altri[217]. Se si seguisse il criterio restrittivo, ritenendo irrilevanti i danneggiamenti di dati e sistemi commessi dagli stessi proprietari, si creerebbe un vuoto di tutela[218]. Per questo motivo, la cerchia degli aventi diritto all'integrità

[210] SARZANA DI S. IPPOLITO C., *La legge di ratifica della Convenzione di Budapest: una "gatta" legislativa frettolosa*, in *Dir. pen. proc*., 2008, n. 12, p. 1562 ss., p. 1566.
[211] PICA G., *Diritto penale delle tecnologie informatiche*, cit., p. 87; TADDEI ELMI G., *Corso di informatica giuridica*, Napoli, 2007, p. 205.
[212] PICA G., *Diritto penale delle tecnologie informatiche*, cit., p. 87.
[213] SALVADORI I., *I danneggiamenti informatici*, in *Diritto penale dell'informatica. Reati della rete e sulla rete*, cit., p. 595 ss., p. 599; PICOTTI L., *Sistematica*, cit. p. 70 s.; CAPPELLINI A., *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici*, in *Cybercrime*, cit., p. 761 ss., p. 777 e 799.
[214] PERRI P., *Sub art. 635-bis c.p.*, in *Commentario breve al codice penale*, cit., p. 2243 ss., p. 2244.
[215] PECORELLA C., *Il diritto penale dell'informatica*, cit., p. 190.
[216] PICOTTI L. *voce Reati informatici*, cit., p. 19.
[217] PECORELLA C., *Il diritto penale dell'informatica*, cit., p. 191.
[218] SALVADORI I., *Il "microsistema" normativo concernente i reati informatici*, cit., p. 216.

di dati, informazioni, programmi e sistemi va necessariamente individuata alla stregua della pluralità di interessi giuridici rilevanti di natura obbligatoria, dunque il concessionario, il legittimo utilizzatore, nonché il concedente e proprietario oppure l'operatore del sistema, legittimato agli interventi che subiscano pregiudizio dal danneggiamento stesso[219].

Per quanto riguarda l'elemento soggettivo, tutti i reati in questione sono puniti a titolo di dolo generico[220].

La prima fattispecie del microsistema è costituita dall'art. 635-*bis* c.p. Oggetto materiale del reato in questione sono i dati, le informazioni e i programmi. Per dati si intendono quelle rappresentazioni di informazioni o concetti rappresentati in modalità idonea ad essere processata da un elaboratore[221]. Per programmi informatici, invece, un insieme coordinato di dati espresso in un linguaggio comprensibile per un elaboratore e strutturati in modo da determinare o consentire il compimento di determinate operazioni, mentre per informazioni delle entità astratte che rilevano solo quando incorporate in un determinato supporto materiale[222]. Vi è però chi evidenzia che la distinzione tra i tre concetti non appare agevole, perché essi tendono a sovrapporsi[223]. In particolare, si è criticata la scelta di mantenere quale oggetto del reato le informazioni, sovrapponibili ai dati e fonte di problemi interpretativi[224].

Le condotte sanzionate consistono nel distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici altrui, ipotesi tutte tra loro alternative[225]. Per distruzione si intende la radicale e definitiva alterazione dell'identità fisica del bene danneggiato, in modo da renderlo inutilizzabile in maniera irrecuperabile per la funzione cui era destinato[226]. Pertanto, costituisce distruzione qualunque azione che comporti la perdita dell'originaria funzione del bene, mentre deterioramento ogni forma di usura dello stesso che ne renda inaffidabile o incoerente il funzionamento[227]. Il deterioramento consiste nella causazione di un peggioramento delle condizioni, anche solo estetiche, purché di evidente percezione, del sistema, dunque nella diminuzione apprezzabile della loro funzione strumentale, utilizzabilità o valore [228].

---

[219] PICOTTI L., *La ratifica della Convenzione Cybercrime*, cit., p. 711.
[220] CAPPELLINI A., *I delitti contro l'integrità dei dati*, cit., p. 793.
[221] PECORELLA C., *Il diritto penale dell'informatica*, cit., p. 75.
[222] *Ibid*., p. 75 e 78.
[223] CAPPELLINI A., *I delitti contro l'integrità dei dati*, cit., p. 778.
[224] SALVADORI I., *Il "microsistema" normativo concernente i reati informatici*, cit., p. 208.
[225] CAPPELLINI A., *I delitti contro l'integrità dei dati*, cit., p. 784.
[226] PICA G., *Diritto penale delle tecnologie informatiche*, cit., p. 88.
[227] *Ibid*., p. 89.
[228] CAPPELLINI A., *I delitti contro l'integrità dei dati*, cit., p. 784.

Le condotte di cancellazione, alterazione e soppressione sono state aggiunte dalla l. 48/2008. La cancellazione consiste nel rendere completamente e definitivamente irriconoscibile il contenuto di dati e programmi informatici[229]. A tal proposito, si evidenzia che ai fini dell'integrazione del reato in esame il fatto che i file cancellati possano essere recuperati non ha alcuna rilevanza[230]. Per quanto riguarda l'alterazione, essa può riguardare tutte quelle attività mediante le quali si modifica il contenuto dei dati o programmi presenti in un sistema informatico o telematico, ad esempio cambiando senza autorizzazione il contenuto di una pagina *web*[231]. La soppressione ricomprende, oltre ai fatti che cagionano un'eliminazione definitiva di dati e che ne fanno venir meno ogni possibilità di recupero sul computer o supporto in cui siano memorizzati, anche quelli che impediscono, seppur temporaneamente, al legittimo titolare di accedervi e di disporne[232].Vi è però chi ha osservato che le stesse ipotesi potevano già rientrare nella condotta di "rendere inservibili in tutto o in parte" punita dalla norma prima della modifica di cui alla suddetta legge[233]. La clausola di chiusura "o rendere tutto o in parte inservibili" è stata eliminata dalla l. 48/2008, scelta che ha sollevato forti perplessità, dato che essa si riferisce solo in parte alle condotte che possono essere riconducibili al deterioramento[234].

Va però evidenziato che, come tutti i reati di danneggiamento, anche esso è a forma libera, visto che la condotta è polarizzata attorno alla produzione causale dell'evento dannoso, senza estrinsecarsi in forme particolari e tassative. Per cui le espressioni in esame debbono intendersi come "cagionare la distruzione, il deterioramento, ecc." e possono essere realizzate sia mediante una condotta attiva che mediante una condotta omissiva[235]. Trattasi, pertanto, di reato di evento, che si consuma nel momento in cui i dati, le informazioni o i programmi sono stati distrutti, deteriorati, alterati, ecc.[236].

---

[229] SALVADORI I., *Il "microsistema" normativo concernente i reati informatici*, cit., p. 210.
[230] V. Cass. pen., sez. V, sentenza 5 marzo 2012, n. 8555, secondo cui «*sembra corretto ritenere conforme allo spirito della disposizione normativa che anche la cancellazione, che non escluda la possibilità di recupero se non con l'uso - anche dispendioso - di particolari procedure, integri gli estremi oggettivi della fattispecie delittuosa. Il danneggiamento che è presupposto della previsione sostanziale, sottospecie del* genus *rappresentato dal reato di danneggiamento di cui all'art. 635 c.p., deve intendersi integrato dalla manomissione ed alterazione dello stato del computer, rimediabili solo con postumo intervento recuperatorio, e comunque non reintegrativo dell'originaria configurazione dell'ambiente di lavoro. Si tratta, dunque, di attività produttiva di danno, in quanto il recupero, ove possibile, comporta oneri di spesa o, comunque, l'impiego di unità di tempo lavorativo*».
[231] PERRI P., *Sub art. 635-bis c.p.*, cit., p. 2244.
[232] SALVADORI I., *Il "microsistema" normativo concernente i reati informatici*, cit., p. 209.
[233] PERRI P., *Sub art. 635-bis c.p.*, cit., p. 2243.
[234] SALVADORI I., *Il "microsistema" normativo concernente i reati informatici*, cit., p. 209.
[235] PICA G., *Diritto penale delle tecnologie informatiche*, cit., p. 88.
[236] *Ibid*., p. 93.

Per quanto riguarda il trattamento sanzionatorio, anche in questo caso, analogamente a quanto avviene per la truffa e la frode informatica, il danneggiamento informatico di cui all'art. 635-*bis* c.p. nella sua ipotesi base è punito con pena identica rispetto al danneggiamento comune. Al co. 2 è poi prevista una circostanza aggravante speciale per il fatto commesso dall'operatore del sistema, che pone gli stessi problemi già esaminati nei paragrafi precedenti con riferimento all'individuazione dell'ambito applicativo di tale nozione[237].

Il problema principale del reato in questione è che la formulazione della norma non consente di individuare facilmente il confine tra comportamenti leciti ed illeciti. Il legislatore italiano, infatti, ha costruito la fattispecie in esame sul modello del danneggiamento tradizionale, senza considerare che a differenza delle ipotesi in cui l'evento ricade su beni materiali, le condotte descritte non hanno un significato naturalistico d'illiceità[238]. Infatti, le ipotesi di distruzione, deterioramento, cancellazione, alterazione o soppressione di informazioni, dati e programmi informatici rappresentano degli "eventi" tecnicamente neutri, che non hanno di per sé alcuna connotazione illecita[239]. Né a tal fine può essere d'aiuto il richiamo all'"altruità", dato che, come sopra esaminato, è esso stesso fuorviante[240]. Non è facile, pertanto, stabilire a priori quali fatti di danneggiamento sono illeciti. Si concorda però con chi sostiene che il disvalore non può essere desunto dalla mera mancanza del consenso dell'avente diritto, pena un'eccessiva dilatazione dell'ambito applicativo della fattispecie[241].

Norma parallela all'art. 635-*bis* c.p. è costituita dall'art. 635-*quater* c.p., che sanziona il danneggiamento di sistemi informatici o telematici. Per quanto riguarda la differenza tra le due fattispecie, essa risiede nella diversità dell'oggetto materiale. In questo caso, infatti, in luogo di dati, informazioni o programmi, esso è costituito dai sistemi informatici o telematici. A tal proposito, la Cassazione ha precisato che il "dato informatico" può essere danneggiato separatamente dalla complessiva apparecchiatura in cui è contenuto, rappresentata dal sistema informatico[242].

La nozione di "sistema informatico" è identica a quella della fattispecie di frode informatica, per cui si ha danneggiamento di un sistema informatico o telematico

[237] PERRI P., *Sub art. 635-bis c.p.*, cit., p. 2243.
[238] PICOTTI L. *voce Reati informatici*, cit., p. 19.
[239] SALVADORI I., *Il "microsistema" normativo concernente i reati informatici*, cit., p. 214.
[240] PICOTTI L. *voce Reati informatici*, cit., p. 19; SALVADORI I., *Il "microsistema" normativo concernente i reati informatici*, cit., p. 216.
[241] SALVADORI I., *Il "microsistema" normativo concernente i reati informatici*, cit., p. 215.
[242] Cass. pen., sez. VI, sentenza 10 giugno 2015, n. 24617.

ogniqualvolta oggetto di aggressione sia il sistema nel suo complesso, ovvero una o più delle sue componenti materiali[243].

Trattasi di reato di evento a forma vincolata, dato che il risultato lesivo deve prodursi "mediante le condotte di cui all'art. 635-*bis* c.p." o attraverso l'introduzione o trasmissione di dati, informazioni o programmi[244]. Le condotte rilevanti ai sensi dell'art. 635-*quater* c.p. sono in gran parte sovrapponibili agli eventi di cui all'art. 635-*bis* c.p., dato il richiamo presente nella fattispecie. Tuttavia, vi sono ulteriori condotte proprie esclusivamente dell'art. 635-*quater* c.p., quali l'introduzione e la trasmissione di dati, informazioni o programmi. Trattasi di aggressioni esclusivamente a carattere logico "a distanza"[245]. In questo modo, rientrano nell'ambito applicativo della fattispecie in questione anche le condotte di danneggiamento dovute a *malware* fatti circolare in rete o appositamente installati nel sistema, che producono uno degli eventi indicati nella norma[246]. Trattasi di condotte alternative tra loro, per cui il reato in questione è una c.d. norma a più fattispecie[247].

I reati divergono anche per quanto riguarda gli eventi. L'art. 635-*quater*, infatti, oltre alla distruzione prevede anche il più generico danneggiamento, in luogo del deterioramento[248]. Inoltre, sanziona anche il fatto di rendere, in tutto o in parte, inservibili sistemi informatici o telematici altrui o di ostacolarne gravemente il funzionamento. L'evento di "rendere in tutto o in parte inservibili" concerne i fatti di alterazione dell'utilizzabilità del bene, in rapporto alla funzione tipica che lo stesso è destinato a soddisfare[249]. La Cassazione ritiene costituisca derivazione della condotta di distruzione o danneggiamento[250]. Nel concetto di inservibilità parziale deve farsi rientrare qualsiasi atto che renda non più utilizzabile anche una singola funzione dell'apparecchio, benché il resto del sistema continui a funzionare[251]. L'ultimo evento è costituito dall'ostacolare gravemente il funzionamento del sistema informatico o telematico. Quest'ultimo costituisce clausola di chiusura che estende la punibilità per sabotaggio informatico anche ai casi in cui l'aggressione logica si limiti a pregiudicare solo parzialmente la funzionalità del sistema[252]. In quest'ultimo caso l'ambito penale è stato limitato a quei fatti che ostacolano "gravemente"

[243] PECORELLA C., *Il diritto penale dell'informatica*, cit., p. 188.
[244] SALVADORI I., *I danneggiamenti informatici*, cit., p. 608.
[245] CAPPELLINI A., *I delitti contro l'integrità dei dati*, cit., p. 788.
[246] PERRI P., *Sub art. 635-quater c.p.*, in *Commentario breve al Codice Penale*, cit., p. 2246 ss., p. 2247.
[247] SALVADORI I., *Il "microsistema" normativo concernente i reati informatici*, cit., p. 211.
[248] PICOTTI L., *La ratifica della Convenzione Cybercrime*, cit., p. 713.
[249] PICA G., *Diritto penale delle tecnologie informatiche*, cit., p. 89.
[250] Cass. pen., sez. II, sentenza 23 dicembre 2016, n. 54715.
[251] PICA G., *Diritto penale delle tecnologie informatiche*, cit., p. 90.
[252] CAPPELLINI A., *I delitti contro l'integrità dei dati*, cit., p. 792.

il funzionamento del sistema. Trattasi di clausola indeterminata che consente di escludere la rilevanza penale dei fatti che producono un'interruzione di lieve entità ad un sistema d'informazione[253]. Per alcuni nell'evento di ostacolo va ricompresa anche l'ipotesi dell'interruzione, seppur non espressamente menzionata dal nostro legislatore[254].

Va però evidenziato che le condotte descritte dall'art. 635-*bis* c.p. e richiamate nell'art. 635-*quater* c.p. finiscono per sovrapporsi agli eventi specificamente descritti in seguito da quest'ultima norma, col risultato che diviene impossibile distinguere tra condotta ed evento[255]. L'unico modo per operare efficacemente una distinzione è riconoscere che le cinque condotte di cui all'art. 635-*bis* c.p. conservino il richiamo che avevano nella sede originaria, dunque siano riferite unicamente a dati, informazioni o programmi[256]. In questo modo l'art. 635-*quater* c.p. finisce per articolarsi su di uno schema con doppio evento, nel quale il c.d. evento intermedio è costituito da uno degli eventi tipici dell'art. 635-*bis* c.p., ovvero il danneggiamento di dati, informazioni o programmi, cui faccia seguito l'evento finale di distruzione, danneggiamento, procurata inservibilità od ostacolo al sistema informatico[257]. Tale tesi ben si concilia con la fenomenologia degli attacchi informatici, dato che prima di danneggiare il sistema solitamente il *malware* opera alterando o danneggiandone i dati.

Dall'ambito di applicazione della norma restano esclusi i c.d. danneggiamenti fisici, ovvero quelli commessi a danno della sola parte *hardware* del sistema informatico, ipotesi che potranno essere sanzionate solo quale danneggiamento tradizionale[258].

Per quanto riguarda il trattamento sanzionatorio, il reato in questione è punito più gravemente rispetto all'art. 635-*bis* c.p. Inoltre, in questo caso è prevista la circostanza aggravante del fatto commesso con violenza alla persona o con abuso della qualità di operatore del sistema. In questo caso, però, si tratta di aggravante ad efficacia comune.

Oltre a queste due fattispecie a tutela dei dati e sistemi informatici "privati", vi sono altre due fattispecie a tutela dei dati e sistemi informatici "pubblici", ovvero gli artt. 635-*ter* e 635-*quinquies* c.p. Questi ultimi, infatti, si differenziano dai due reati appena esaminati perché sono volti a tutelare dati e sistemi "di pubblica utilità"[259]. In questi casi poi, come

[253] SALVADORI I., *Il "microsistema" normativo concernente i reati informatici*, cit., p. 213.
[254] PICOTTI L., *La ratifica della Convenzione Cybercrime*, cit., p. 713.
[255] *Ibid*.
[256] CAPPELLINI A., *I delitti contro l'integrità dei dati*, cit., p. 790.
[257] PICOTTI L., *La ratifica della Convenzione Cybercrime*, cit., p. 713 s.; CAPPELLINI A., *I delitti contro l'integrità dei dati*, cit., p. 790.
[258] SALVADORI I., *Il "microsistema" normativo concernente i reati informatici*, cit., p. 214.
[259] PICOTTI L., *La ratifica della Convenzione Cybercrime*, cit., p. 715.

sopra accennato, non è richiesto che i dati ed i sistemi siano "altrui". Il legislatore, tuttavia, nell'art. 635-*ter* c.p. fa riferimento alle informazioni, dati o programmi informatici "utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità", mentre all'art. 635-*quinquies* c.p. unicamente ai sistemi informatici "di pubblica utilità". Dunque, in modo inopportuno le due norme in questione non sono state formulate in maniera omogenea. Va però osservato che la formula generale "di pubblica utilità" appare idonea a ricomprendere anche le situazioni menzionate dal solo art. 635-*ter* c.p., anche perché è difficile individuare il rapporto di "pertinenza" richiesto dalla norma in questione[260]. Per pubblica utilità si intende la destinazione al servizio di una collettività indifferenziata e indeterminata di persone[261].

La distinzione tra art. 635-*ter* e art. 635-*quinquies* c.p. è analoga a quella sopra evidenziata per le fattispecie di danneggiamenti informatici di dati e sistemi "privati": oggetto materiale del primo reato sono dati, informazioni e programmi, mentre oggetto del secondo sono i sistemi informatici o telematici[262].

A differenza degli artt. 635-*bis* e 635-*quater* c.p., gli artt. 635-*ter* e 635-*quinquies* c.p. sono costruiti come delitti di attentato, per cui la soglia di rilevanza penale è anticipata[263]. Dunque, in entrambi i casi il tentativo non è configurabile[264]. L'art. 635-*ter* c.p. prevede che le condotte aggressive debbano essere dirette a cagionare uno dei cinque eventi propri dell'art. 635-*bis* c.p. Si tratta di reato di pericolo che si consuma già al momento della commissione di atti diretti a produrre uno degli effetti indicati nella norma[265]. Il co. 2, invece, è un'ipotesi di reato aggravato dall'evento, nel caso in cui uno degli effetti indicati dalla norma si verifichi[266]. Alcuni autori evidenziano che la disposizione in questione è formulata come reato autonomo, dato che la pena, più del doppio rispetto a quella prevista dal co. 1, è stabilita in modo indipendente[267]. Ciò, peraltro, sembra trovare conferma nel fatto che pure qui è prevista una circostanza aggravante ad efficacia comune, se il fatto sia commesso con violenza alla persona, minaccia o abuso della qualità di operatore del sistema, circostanza che appare essere applicabile sia al co. 1 che al co. 2. Si ritiene, però, inutile il richiamo alla

[260] *Ibid*.
[261] CAPPELLINI A., *I delitti contro l'integrità dei dati*, cit., p. 800.
[262] *Ibid*.
[263] FUMO M., *La condotta nei reati informatici*, in *Arch. Pen*., 2013, n. 3, p. 771 ss., p. 783.
[264] CAPPELLINI A., *I delitti contro l'integrità dei dati*, cit., p. 805.
[265] PERRI P., *Sub art. 635-ter c.p.*, in *Commentario breve al Codice Penale*, cit., p. 2245 ss., p. 2245.
[266] *Ibid*.
[267] PICOTTI L., *La ratifica della Convenzione Cybercrime*, cit., p. 715.

violenza alla persona, trattandosi di condotte volte a danneggiare il *software*, per cui nella quasi totalità dei casi i criminali informatici agiscono da remoto.

L'art. 635-*quinquies* c.p., invece, sanziona "il fatto di cui all'art. 635-*quater* c.p." diretto a realizzare uno degli eventi di danno descritti nella norma, ovvero distruggere, danneggiare, rendere in tutto o in parte inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento. Data l'impossibilità di interpretare il "fatto" in senso letterale, si può affermare come le condotte del reato in parola siano dirette a cagionare uno dei quattro eventi "finali" già parte dell'art. 635-*quinquies* c.p.[268]. Anche in questo caso al co. 2 è prevista un'ipotesi di reato aggravato dall'evento, nonché la circostanza aggravante ad efficacia comune per il fatto commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema.

Si concorda con chi ritiene che il settore dei danneggiamenti informatici sia caratterizzato da eccessiva sovrabbondanza di disposizioni normative, influenzate dall'eccessivo timore di lacune normative[269]. Nonostante questo, va evidenziato che l'art. 4 della direttiva 2013/40/UE prevedeva espressamente l'incriminazione delle condotte di "*ostacolare gravemente o interrompere il funzionamento di un sistema di informazione*", compiute anche "*rendendo inaccessibili i dati informatici*". Tuttavia, l'art. 19 della citata legge di attuazione della menzionata direttiva non ha aggiunto tali condotte in nessuna delle fattispecie elencate, nonostante la Commissione europea avesse già nel 2017 evidenziato che la normativa italiana in materia non rispettava il contenuto della Direttiva[270]. Va infatti ribadito che il co. 3 dell'art. 420 c.p., che puniva l'ipotesi aggravata del delitto di "attentato informatico" qualora dal fatto di reato fosse derivata l'interruzione, anche parziale, del funzionamento dell'impianto o del sistema informatico attaccato, è stata abrogata dalla citata l. 18 marzo 2008, n. 48. Inoltre, gli odierni artt. 635-*quater* e 635-*qunquies* c.p. non fanno alcun riferimento all'interruzione o al fatto di rendere inaccessibili i dati. Dunque, è opportuno che il legislatore intervenga quanto prima per introdurre (o reintrodurre[271]) la punibilità delle condotte in esame, data la massiccia diffusione dei *malware* di tipo *ransomware*, volti proprio ad impedire agli utenti di accedere liberamente al proprio sistema

[268] CAPPELLINI A., *I delitti contro l'integrità dei dati*, cit., p. 804.
[269] PICOTTI L. *voce Reati informatici*, cit., p. 16.
[270] *Relazione della Commissione al Parlamento europeo e al Consiglio che valuta in che misura gli Stati membri hanno adottato le misure necessarie per conformarsi alla direttiva 2013/40/UE relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio*, disponibile *online* al sito https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52017DC0474&qid=1506754119753&from=IT
[271] Come sostenuto anche da CIVELLO CONIGLIARO S., *La nuova tutela penale europea dei sistemi di informazione*, cit., p. 4.

informatico, se non a seguito del pagamento di un riscatto. Nonostante ciò, è possibile ritenere che l'utilizzo di un *ransomware* in molti casi già rientri nell'ambito applicativo delle fattispecie in esame, qualora il programma malevolo abbia pregiudicato l'utilizzo o il funzionamento dei programmi o del sistema[272]. Nel caso in cui, invece, il *ransomware* abbia semplicemente impedito all'utente di utilizzare il sistema informatico nel suo complesso, senza provocare la totale distruzione dello stesso, può essere considerato "grave ostacolo al suo funzionamento", evento punito ai sensi dell'art. 635-*quater* c.p.

L'individuazione dei rapporti tra i reati di cui al microsistema è resa agevole dalla presenza delle clausole di sussidiarietà espressa, che ha proprio la funzione di regolare i rapporti tra i quattro reati in questione, facendo salva l'applicazione del reato più grave, tant'è che l'art. 635-*quinquies* c.p., ovvero la fattispecie punita più gravemente, ne è priva[273].

Problematici, invece, sono i rapporti con le altre fattispecie poste al di fuori del microsistema. Infatti, va evidenziato che l'alterazione del sistema informatico è condotta sanzionata anche dall'art. 640-*ter* c.p. A tal proposito, la giurisprudenza ha osservato che il reato di frode informatica si differenzia da quello di danneggiamento di dati informatici perché, nel primo, il sistema informatico continua a funzionare, benché in modo alterato rispetto a quello programmato, mentre nel secondo l'elemento materiale è costituito dal mero danneggiamento del sistema informatico o telematico, e, quindi, da una condotta finalizzata ad impedire che il sistema funzioni[274]. I due reati, dunque, sono tra loro incompatibili.

Rispetto ai danneggiamenti informatici è opportuno esaminare anche i controversi rapporti tra le diverse fattispecie di danneggiamento informatico e il delitto di accesso abusivo a un sistema informatico ex art. 615-*ter* c.p., con riferimento in particolare all'aggravante specifica di cui al co. 2, numeri due e tre. Come già esaminato (v. *supra*, cap. II par. 2), il numero due sanziona l'accesso abusivo commesso con violenza sulle cose, concetto, quest'ultimo, nel quale, ai sensi dell'art. 392 co. 3 c.p., rientrano l'alterazione, la modifica o la cancellazione totale o parziale nonché l'impedimento o il turbamento del funzionamento di un sistema informatico o telematico. Il numero tre, invece, prevede un evento aggravatore quando, come conseguenza dell'accesso abusivo, derivi la distruzione o il danneggiamento del sistema informatico. A tal proposito, va ricordato che il delitto di cui all'art. 635-*bis* c.p., che prevede la clausola di sussidiarietà espressa, è punito meno

[272] Così anche LUBERTO M., "Sex-torsion" *via* web *e minaccia a mezzo* ransomware, cit., p. 757 s.; BRIZZI F., *I profili penali del ransomware*, cit., p. 4.
[273] CAPPELLINI A., *I delitti contro l'integrità dei dati*, cit., p. 795.
[274] Cass. pen., sez. II, sentenza 1 dicembre 2016, n. 54715.

gravemente rispetto alla fattispecie aggravata di cui al n. 2 del co. 2 dell'art. 615-*ter* c.p., per cui si può ritenere che qualora la violenza sul sistema informatico sia strumentale all'accesso abusivo il fatto debba essere punito unicamente ai sensi dell'art. 615-*ter* co. 2 n. 2 c.p., senza che vi sia concorso tra le fattispecie[275]. Tuttavia, la nozione di violenza sulle cose prevista dall'art. 392 co. 3 c.p. è più ristretta rispetto a quella desumibile dall'art. 635-*bis* c.p., perché esclude dagli oggetti materiali le informazioni e i dati, oggetto, invece, del reato di danneggiamento informatico[276]. Inoltre, il requisito della violenza sulle cose ricorre soltanto nelle specifiche ipotesi di alterazione, modificazione o cancellazione di un programma informatico e di impedimento o turbamento del funzionamento di un sistema informatico o telematico e non in quelle della distruzione, del deterioramento e della soppressione di programmi informatici[277]. In questi ultimi casi non vi potrà essere sussunzione nella fattispecie aggravata di cui all'art. 615-*ter* co. 2 n. 2 c.p., ma si dovrà necessariamente applicare sia l'art. 635-*bis* c.p. che l'ipotesi base di cui art. 615-*ter* c.p., in quanto quest'ultima fattispecie è punita meno gravemente e non è in rapporto di specialità con la prima.

Tale soluzione, tuttavia, non soddisfa perché finisce per creare ingiustificate disparità di trattamento rispetto a fatti sostanzialmente identici[278]. In questo caso, dunque, la rigorosa applicazione del principio di specialità dà adito a frizioni col principio di uguaglianza, perché sanziona in maniera differente fatti connotati da uguale disvalore.

Meno problematico, invece, è il rapporto tra l'art. 635-*bis* c.p. e il reato aggravato dall'evento di cui all'art. 615-*ter* co. 2 n. 3 c.p. In questo caso, infatti, si può ritenere che quest'ultima fattispecie si applichi ai soli casi in cui l'evento aggravatore del danneggiamento non sia voluto dal soggetto agente; dunque, qualora il danneggiamento non costituisca la finalità dell'introduzione in un sistema informatico, bensì semplicemente si sia verificato in conseguenza dell'accesso non autorizzato, secondo le regole di imputazione di cui all'art. 59 c.p.

Per quanto riguarda, invece, il reato di cui all'art. 635-*quater* c.p. la questione è differente, perché qui la clausola di sussidiarietà non può trovare applicazione in relazione all'art. 615-*ter* c.p., dato che le pene sono identiche. Si può però fare riferimento al criterio distintivo della diversità dell'elemento soggettivo e ritenere che si applichi l'art. 615-*ter* co.

[275] Così anche SALVADORI I., *Danneggiamenti informatici*, cit., p. 620.
[276] CAPPELLINI A., *I delitti contro l'integrità dei dati*, cit., p. 823.
[277] In tal senso SALVADORI I., *Il "microsistema" normativo concernente i reati informatici*, cit., p. 215 e 234.
[278] SALVADORI I., *Danneggiamenti informatici*, cit., p. 620.

2 n. 3 c.p. qualora il danneggiamento costituisca una conseguenza non voluta dell'accesso abusivo, mentre in caso contrario si applica il reato di danneggiamento informatico ex art. 635-*quater* co. 2 c.p., in concorso con la fattispecie base di accesso abusivo. Anche con riferimento ai reati di danneggiamento informatico di cui agli artt. 635-*ter* e 635-*quinquies* c.p. è difficile individuare i rapporti col reato di cui ai co. 2 n. 2 e co. 3 dell'art. 615-*ter* c.p. per il fatto commesso su sistemi informatici o telematici di interesse militare, di ordine pubblico o interesse pubblico. Infatti, il trattamento sanzionatorio previsto è identico e la presenza della clausola di chiusura «*o comunque di interesse pubblico*» nel co. 3 dell'art. 615-*ter* c.p. rende difficile ipotizzare che tale norma sia in rapporto di specialità rispetto ai reati di danneggiamento informatico sopra elencati[279]. In ogni caso, qualora si aderisse alla tesi della specialità dell'art. 615-*ter* co. 2 e 3 c.p., vi sarebbe lo stesso identico problema già segnalato con riferimento all'art. 635-*bis* c.p., ovvero che nei casi in cui l'oggetto materiale del danneggiamento sia diverso rispetto a quelli elencati nel co. 3 dell'art. 615-*ter* c.p. si dovrebbe necessariamente concludere per la sussistenza del concorso tra gli artt. 635-*ter o* 635-*quinquies* c.p. e l'art. 615-*ter* c.p. nella sua ipotesi base, dunque paradossalmente sanzionando più gravemente fatti connotati da minor disvalore. Tuttavia, anche in questo caso si può far riferimento al criterio della diversità dell'elemento soggettivo e ritenere che qualora il danneggiamento sia una conseguenza non voluta dell'accesso abusivo si applicherà unicamente l'art. 615-*ter* co. 3 c.p.[280].

Va poi evidenziato che il microsistema normativo concernente i danneggiamenti informatici comprende l'esaminata fattispecie di cui all'art. 615-*quinquies* c.p., che, come sopra evidenziato, sanziona le condotte prodromiche alla commissione di un effettivo danneggiamento informatico (v. *supra*, cap. II, par. 5). Vanno, dunque, esaminati i rapporti tra i reati di danneggiamento informatico di cui agli artt. 635-*bis*, *ter*, *quater* e *quinquies* e il diverso reato di cui all'art. 615-*quinquies*. c.p. Tale ultima norma, infatti, analogamente all'art. 615-*quater* c.p., sanziona le condotte prodromiche alla commissione di un danneggiamento informatico, ma non contiene alcuna clausola di sussidiarietà a favore dei più gravi delitti di danneggiamento. Se si utilizza unicamente il criterio della specialità, anche in questo caso si deve ritenere che, in caso di avvenuto danneggiamento, tale ultimo reato possa concorrere o con il reato di cui all'art. 635-*bis* c.p. in caso di avvenuto danneggiamento di informazioni, dati o programmi informatici altrui (o 635-*ter* se utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti o comunque di pubblica utilità), o

[279] Così anche CAPPELLINI A., *I delitti contro l'integrità dei dati*, cit., p. 808.
[280] *Ibid*.

con quello di cui all'art. 635-*quater* c.p. in caso di danneggiamento o ostacolo al funzionamento di sistemi informatici o telematici altrui (o art. 635-*quinquies* se utilizzato dallo Stato o da altro ente pubblico o ad essi pertinenti o comunque di pubblica utilità). Nonostante la presenza negli artt. 635-*bis*, 635-*ter* e 635-*quater* c.p. della clausola di sussidiarietà, essa non può trovare applicazione nei confronti dell'art. 615-*quinquies*, poiché fattispecie punita meno gravemente. I reati di danneggiamento, inoltre, si consumano in momenti fisiologicamente diversi rispetto a quello di cui all'art. 615-*quinquies* c.p., per cui, secondo il criterio della specialità, si deve escludere il concorso apparente a favore del concorso di reati[281].

Anche in questo caso, tuttavia, valgono le stesse considerazioni sopra esposte con riferimento all'art. 615-*quater* c.p., essendo anche l'art. 615-*quinquies* c.p. reato di pericolo che punisce comportamenti prodromici al danneggiamento informatico[282]. Anche qui, dunque, si puniscono le diverse fasi dello stesso fenomeno criminoso, con disvalore penale sostanzialmente omogeneo, per cui, utilizzando il diverso criterio di consunzione-assorbimento, ben si potrebbe ritenere che l'art. 615-*quinquies* c.p. rimanga assorbito dalla fattispecie di danneggiamento informatico, trattandosi di reato ostacolo rispetto alla realizzazione di offese all'integrità di dati o sistemi informatici[283]. Tale tesi, peraltro, troverebbe conferma nella diversità dei limiti edittali previsti dalle fattispecie di cui agli artt. 635-*bis*, *ter*, *quater* e *quinquies* c.p. rispetto a quella dell'art. 615-*quinquies* c.p. Sussiste però anche qui il problema della diversa procedibilità dei reati, dato che l'art. 615-*quinques* è procedibile d'ufficio, per cui, anche ad accogliere la tesi dell'assorbimento, in caso di rimessione di querela per il danneggiamento informatico l'autore del fatto si troverebbe comunque a rispondere del reato di cui all'art. 615-*quinquies* c.p.[284].

Va esaminato anche il rapporto con il reato di estorsione. Infatti, come sopra evidenziato, l'impiego di un *ransomware* può astrattamente integrare sia la fattispecie di estorsione che quella di danneggiamento. A tal proposito, vi è chi ritiene che i reati di danneggiamento informatico di cui agli artt. 635-*quater* e 635-*quinquies* c.p. possano

[281] PICA G., *Diritto penale delle tecnologie informatiche*, cit., p. 97.
[282] PICOTTI L., *La ratifica della Convenzione* Cybercrime, cit., p. 708; SALVADORI I., *I reati contro la riservatezza informatica*, cit., p. 704
[283] In tali termini anche SALVADORI I., *Danneggiamenti informatici*, cit., p. 621; in CAPPELLINI A., *I delitti contro l'integrità dei dati*, p. 817.
[284] Cft. PAGLIARO A., voce *Concorso di norme penali*, cit., p. 552, che evidenzia che poiché nell'ipotesi della consunzione l'inapplicabilità di una disposizione si verifica in seguito all'assorbimento dello scopo da essa perseguito nello scopo cui tende l'altra norma, la consunzione va esclusa qualora l'interesse di portata maggiore non sia effettivamente tutelato, per cui se il reato più grave non è stato contestato o non è procedibile non si applica alcun assorbimento.

ritenersi assorbiti nel reato di estorsione, posto che la violenza di cui all'art. 629 c.p. coincide con la nozione di violenza sulle cose di cui all'art. 392 co. 3 c.p.[285]. Tale tesi trova conferma nel principio affermato dalla Cassazione secondo cui la condotta di violenza costituisce nucleo essenziale del delitto di estorsione, per cui qualora non rechi una lesione personale, perché ad esempio si tratta di violenza reale, rimane interamente assorbita in quest'ultimo reato[286]. Tale principio può trovare applicazione anche per i reati di cui agli artt. 635-*bis* e 635-*ter* c.p., nonostante, come evidenziato, le condotte punite da questi ultimi non possano sempre rientrare nel concetto di violenza informatica di cui all'art. 392 c.p., dato che quest'ultima norma menziona unicamente i programmi ed i sistemi.

5. Concorso di reati

Come evidenziato, per effettuare la disposizione patrimoniale in luogo del titolare della somma di denaro, o per danneggiare il sistema, il criminale informatico deve prima compiere una serie di passaggi intermedi. Per questo caso si pone il problema dell'eventuale concorso di più reati.

Se il reo, dopo aver illecitamente ottenuto le *password* altrui ed effettuato un accesso abusivo, consegue anche un ingiusto profitto con altrui danno, non avrà commesso solo il reato di frode informatica di cui all'art. 640-*ter* c.p., ma anche quello di cui all'art. 615-*ter* c.p. La giurisprudenza, anche recente, ritiene pacificamente ammissibile il concorso tra la frode informatica e il reato di accesso abusivo ex art. 615-*ter* c.p., evidenziando che i due reati tutelano beni giuridici diversi, ovvero il patrimonio il primo e la riservatezza informatica il secondo[287]. Le condotte sanzionate, inoltre, sono tra loro in rapporto di eterogeneità, elemento, questo, che per il criterio della specialità è sicuro indice della configurabilità del concorso di reati. Altre pronunce giurisprudenziali però, seppure ad altri fini, hanno affermato che il bene giuridico tutelato dalla fattispecie di frode informatica non è unicamente il patrimonio, ma va esteso anche alla tutela della riservatezza dei dati, qualificandolo come "*illecito plurioffensivo*"[288]. In tale prospettiva, dunque, si può mettere

[285] LUBERTO M., "Sex-torsion" *via* web *e minaccia a mezzo* ransomware, cit., p. 758.
[286] Cass. pen., sez. II, sentenza 23 aprile 2019, n. 17427.
[287] v. da ultimo Cass. pen., sez. V, sentenza 8 giugno 2020, n. 17360. In senso conforme anche: Cass. pen., sez. II, sentenza 17 giugno 2019, n. 26604; Cass. pen., sez. V, sentenza 16 gennaio 2009, n. 1727; Cass. pen., sez. V, sentenza 27 gennaio 2004, n. 2672.
[288] v. Cass. pen., sez. II, sentenza 15 aprile 2011, n. 17748, che nel definire i rapporti tra il reato di frode informatica e di indebito utilizzo di carta di credito così evidenzia «*Il bene giuridico tutelato dal delitto di frode informatica, non può, dunque, essere iscritto esclusivamente nel perimetro della salvaguardia del patrimonio del danneggiato, come pure la collocazione sistematica lascerebbe presupporre, venendo*

in discussione l'assunto secondo cui i due reati devono necessariamente concorrere perché a tutela di beni giuridici diversi. È pur vero che, a differenza di quanto evidenziato sopra per gli artt. 615-*quater* e 615-*quinquies* c.p., non sempre l'accesso abusivo ad un sistema informatico o telematico si accompagna ad una frode informatica, in quanto, in assenza di manipolazione del sistema, che è un elemento costitutivo della frode informatica, si configura unicamente l'accesso abusivo[289]. Inoltre, tra i due reati vi può essere concorso solo se la condotta tipica ha riguardato un sistema protetto da misure di sicurezza, altrimenti l'art. 615-*ter* c.p. non potrebbe neppure astrattamente configurarsi[290]. Tuttavia, sono comunque numerose le ipotesi in cui a seguito di un accesso abusivo il soggetto consegua un ingiusto profitto compiendo ulteriori disposizioni attuate mediante un intervento senza diritto sui dati, ulteriore modalità di commissione del reato.

In tali ipotesi resta il problema dell'individuazione del rapporto tra i due reati, perché l'accesso abusivo diviene presupposto necessario e imprescindibile per la commissione della successiva frode informatica, dando così vita ad una progressione criminosa caratterizzata da disvalore penale sostanzialmente omogeneo, soprattutto se si considera il reato di cui all'art. 640-*ter* c.p. come illecito plurioffensivo. Se, poi, si considera che per compiere un accesso abusivo è necessario anche procurarsi i relativi codici di accesso, secondo il criterio della specialità, poiché le condotte sono tra loro eterogenee, vi sarebbe il concorso tra ben tre norme, ovvero gli artt. 640-*ter*, 615-*ter* e 615-*quater* c.p. Questo cumulo però comporta una notevole sproporzione della pena[291]. Esigenze di giustizia sostanziale impongono un ripensamento e, quindi, l'utilizzo del diverso criterio dell'assorbimento. D'altra parte, vi è un significativo ostacolo a ritenere che l'art. 615-*ter* c.p. possa ritenersi assorbito nel delitto di frode informatica, ovvero il trattamento sanzionatorio identico nel massimo stabilito per le due fattispecie nelle loro ipotesi base, per cui si deve necessariamente concludere per la configurabilità del concorso di reati tra accesso abusivo e frode informatica.

Va però evidenziato che al co. 3 dell'art. 640-ter c.p. è prevista la circostanza

---

chiaramente in discorso anche l'esigenza di salvaguardare la regolarità di funzionamento dei sistemi informatici - sempre più capillarmente presenti in tutti i settori più importanti della vita economica, sociale, ed istituzionale del Paese - la tutela della riservatezza dei dati, spesso sensibili, ivi gestiti, e, infine, aspetto non trascurabile, la stessa certezza e speditezza del traffico giuridico fondata sui dati gestiti dai diversi sistemi informatici». In senso conforme anche Cass. pen. sez. II, sentenza 30 ottobre 2019, n. 50395; Cass. pen., sez. II, sentenza 24 settembre 2018, n. 41013; Cass. pen. sez. V, sentenza 3 luglio 2012, n. 43729. In dottrina v. FIANDACA G., MUSCO E., *Diritto penale, PS*, cit., p. 209; PICOTTI L., *Sistematica dei reati informatici*, cit., p. 55; MARGIOCCO M., *Frode informatica*, cit., p. 1108, secondo cui la fattispecie in esame tutela anche la regolarità del funzionamento dei sistemi informatici e la riservatezza che accompagna l'utilizzatore.

[289] PARODI C., *I reati patrimoniali*, cit., p. 103 ss., p. 108; MINICUCCI G., *Le frodi informatiche*, cit., p. 843

[290] SCOPINARO L., *Furto di dati e frode informatica*, in *Dir. pen. proc*., 2007, n. 3, p. 364 ss., p. 371.

[291] *Ibid*., p. 372.

aggravante ad effetto speciale della frode informatica commessa con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti. Nell'ambito di una fattispecie complessa come la frode informatica commessa con sostituzione d'identità digitale, si configurerebbe quindi un concorso col reato di cui all'art. 615-*ter* c.p.[292]. È però vero che l'art. 615-*ter* c.p. fa riferimento alle "misure di sicurezza", mentre il co. 3 dell'art. 640-*ter* c.p. all' "identità digitale", ovvero ad elementi oggettivi che appaiono diversi. Sembrerebbe, dunque, che le condotte sanzionate dalle due norme siano tra loro in rapporto di eterogeneità. Tuttavia, come sopra evidenziato, il legislatore penale non ha fornito una definizione di identità digitale, per cui rimangono ancora ignoti i limiti e la portata applicativa di questa nozione[293]. Se però, come detto sopra, si intende l'identità digitale come le credenziali in uso in un sito *web* è facile intuire che l'"indebito utilizzo" dell'identità digitale finisce per coincidere con la violazione delle misure di sicurezza per l'accesso al sistema o per l'acquisizione di dati e informazioni[294] e, dunque, l'elemento materiale tra l'aggravante in questione e la fattispecie di cui all'art. 615-*ter* c.p. sarebbe identico. Pertanto, in presenza di unità naturalistica della condotta, si può ritenere che tra le due norme vi sia concorso soltanto apparente, a favore dell'applicazione della sola fattispecie di cui all'art. 640-*ter* co. 3 c.p., speciale poiché l'aggravante in questione presenta tutti gli elementi costitutivi dell'accesso abusivo e costituisce elemento specializzante della frode informatica[295]. Inoltre, per quanto riguarda i beni giuridici tutelati, sebbene l'indebito utilizzo d'identità così come costruito nel comma in questione risulti ontologicamente legato alla frode informatica, esso ha comunque una connotazione più ampia rispetto alla mera tutela del patrimonio[296], perché può essere realizzato per ledere l'onore o la reputazione del soggetto ed in generale il diritto all'identità personale.

Nonostante sia indubbio che identità digitale e riservatezza informatica non siano concetti identici[297], anche se vi è chi ritiene che in realtà il diritto alla riservatezza altro non

[292] MALGIERI G., *Il furto di "identità digitale": una tutela "patrimoniale" della personalità*, in R. Flor, D. Falcinelli, S. Marcolini (a cura di), *La giustizia penale nella rete. Le nuove sfide della società dell'informazione nell'epoca di Internet*, Milano, 2015, p. 37 ss., p. 56.
[293] PISTORELLI L., *Relazione Ufficio del Massimario Cassazione*, n. III/01/2013 del 22 agosto 2013, p. 7, consultabile *online* al sito www.penalecontemporaneo.it
[294] così FLOR R., *La legge penale nello spazio*, cit., p. 171.
[295] MALGIERI G., *La nuova fattispecie di "indebito utilizzo dell'identità digitale*, cit., p. 144.
[296] FLOR R., *La legge penale nello spazio*, cit., p. 171.
[297] Cft. CASSANO G., *Contenuto e limiti del diritto all'identità personale*, cit., p. 121, che evidenzia che da una parte vi è l'esigenza che la rappresentazione ad altri della propria identità risponda a criteri di verità oggettiva senza false rappresentazioni o attribuzioni, mentre dall'altra c'è l'esigenza che aspetti della propria persona rimangano sconosciuti, per cui si tratta di beni giuridici diversi dettati per fini diversi.

sia se non una forma del bene giuridico dell'identità[298], il bene giuridico tutelato dalle due fattispecie è sostanzialmente omogeneo, dato che l'aggravante di cui al co. 3 dell'art. 640-*ter* c.p. punisce l'illecita apprensione e l'utilizzo abusivo dei dati identitari che si voleva mantenere riservati a determinati fini[299]. Per questo motivo, si può ritenere che l'art. 640-*ter* co. 3 c.p. sia norma speciale ex art. 15 c.p., rispetto al reato di cui all'art. 615-*ter* c.p. e che, dunque, le due fattispecie non concorrano tra loro.

A identiche conclusioni si può giungere anche con riferimento al rapporto tra il reato di frode informatica aggravato dal furto o dall'indebito utilizzo di identità digitale e l'art. 615-*quater* c.p., che, come evidenziato, costituisce reato di pericolo volto alla criminalizzazione di condotte che costituiscono la premessa per la realizzazione di più gravi reati. Quanto detto sopra per l'art. 615-*ter* c.p. a maggior ragione vale per quest'ultima fattispecie, anche perché l'acquisizione delle credenziali altrui è proprio una delle fasi del complesso fenomeno del furto di identità[300]. Infatti, l'aggravante in questione sanziona proprio il "furto" d'identità digitale. Se, come evidenziato, l'identità digitale consiste nel profilo abilitativo personale per la fruizione o l'accesso a determinati spazi informatici o servizi nel *cyberspace*[301] e se tale "furto", essendo l'identità un bene immateriale, deve essere inteso come un'illecita apprensione delle componenti essenziali dell'identità digitale, quali nome utente e *password*, è evidente che la condotta sanzionata dalle due norme è identica. Per questo si può ritenere che la fattispecie aggravata di cui al co. 3 dell'art. 640-*ter* c.p. sia speciale anche rispetto al reato di cui all'art. 615-*quater* c.p., dato che, a differenza di quest'ultimo, accede ad una frode informatica consumata. Si può, dunque, propendere anche in questo caso per l'esclusione del concorso di reati e per l'applicazione del solo art. 640-*ter* co. 3 c.p.[302].

In ogni caso, anche qualora non si ritenga sussistente un vero e proprio rapporto di specialità in astratto, si può comunque, applicando il criterio dell'assorbimento, ritenere che

---

[298] Così FINOCCHIARO G., *La protezione dei dati personali e la tutela dell'identità*, in G. Finocchiaro, F. Delfini (a cura di), *Diritto dell'informatica*, Milano, 2014, p. 151 ss., p. 155. In giurisprudenza v. Cass. civ., sez. I, sentenza 22 giugno 1985, n. 3769.

[299] MALGIERI G., *La nuova fattispecie di "indebito utilizzo d'identità digitale". Problemi interpretativi*, p. 147.

[300] In tal senso v. FLOR R., *Phishing, identity theft e identity abuse*, cit., p. 899, che evidenzia come l'illecita acquisizione di codici d'accesso costituisce elemento strutturale del più ampio fenomeno criminale dell'*identity related fraud*.

[301] Così FLOR R., *La legge penale nello spazio*, cit., p. 169

[302] Nello stesso senso MINICUCCI G., *Le frodi informatiche*, cit., p. 843, che, tuttavia, non ritiene le due fattispecie in rapporto di specialità, ma esclude il concorso di reati in quanto ritiene che l'art. 615-*quater* c.p., essendo un reato-ostacolo rivolto alla criminalizzazione di condotte che costituiscono la premessa per la realizzazione di più gravi fattispecie, debba essere assorbito nella fattispecie di frode informatica aggravata dal furto o indebito utilizzo dell'identità digitale.

l'art. 640-*ter* co. 3 c.p., in ragione del suo elevato trattamento sanzionatorio e della sostanziale omogeneità dei beni giuridici tutelati, sia norma idonea ad assorbire anche il disvalore dei reati di cui agli artt. 615-*ter* e 615-*quater* c.p.

Non solo, ma dato l'elevato trattamento sanzionatorio della nuova circostanza aggravante del trasferimento non consentito di un valore patrimoniale, che come esaminato si applica alla quasi totalità delle frodi informatiche, si può oggi ritenere che la frode informatica aggravata o pluriaggravata costituisca reato complesso, idoneo ad assorbire il disvalore di tutti i reati antecedentemente commessi. Infatti, come sottolineato recentemente dalle Sezioni Unite[303], il fatto che tra le diverse norme non sussista una relazione di specialità in astratto non può escludere la configurabilità del reato complesso, perché altrimenti si arriverebbe ad una sostanziale abrogazione dell'art. 84 c.p.

L'ulteriore problema esaminato dalla dottrina attiene al rapporto tra l'art. 494 c.p. e il nuovo co. 3 dell'art. 640-*ter* c.p. Prima dell'introduzione della menzionata circostanza aggravante di cui al co. 3 dell'art. 640-*ter* c.p., si riteneva che il reato di sostituzione di persona potesse concorrere con la frode informatica, analogamente a quanto avviene per la truffa comune[304]. La clausola di sussidiarietà presente nel delitto di sostituzione di persona, infatti, attiene unicamente agli altri delitti contro la fede pubblica. Né si dubita della possibilità di commettere il reato di sostituzione di persona in *Internet*[305]. Il problema dei rapporti tra queste due fattispecie si ripropone oggi in modo diverso a seguito dell'introduzione dell'aggravante di cui al co. 3 dell'art. 640-*ter* c.p. A tal proposito, va specificato che, già prima dell'entrata in vigore della sopra menzionata aggravante, una parte della dottrina riteneva la norma di cui all'art. 494 c.p. non idonea a sanzionare il furto di identità digitale[306]. In particolare, si evidenziava che il "furto d'identità digitale" consiste nell'illecita apprensione dell' «*insieme di dati che permettono di ricollegare un documento*

[303] Cass. pen., sez. un., sentenza 15 luglio 2021, n. 38402.
[304] CIPOLLA P., *Social network, furto di identità e reati contro il patrimonio*, in *Giur. merito*, 2012, n. 12, p. 2672 ss., p. 2677, che evidenzia come i due reati siano posti a tutela di differenti beni giuridici; CAJANI F., *La tutela penale dell'identità digitale*, cit., p. 1098. In giurisprudenza v. Cass. pen. sez. II, sentenza 11 agosto 2020, n. 23760; Cass. pen. sez. II, sentenza 24 settembre 2018, n. 41013.
[305] V. *ex multis* Cass. pen., sez. V, sentenza 23 luglio 2020, n. 22049; Cass. pen., sez. V, sentenza 19 luglio 2018, n. 33862; Cass. pen., sez. V, sentenza 23 aprile 2014, n. 25774; Cass. pen., sez. III, sentenza 15 dicembre 2011, n. 12479 Cass. pen., sez. V, sentenza 8 novembre 2007, n. 46674.
[306] Così FLOR R., *phishing, identity theft e identity abuse*, cit., p. 900: «*L'uso online degli strumenti identificativi di una persona reale, consistenti nelle credenziali di autenticazione per l'accesso a sistemi informatici o spazi virtuali esclusivi, non corrisponde all'attribuzione tipizzata di un "falso nome", un "falso stato" o una "qualità a cui la legge attribuisce effetti giuridici". Nel caso in esame, infatti, non viene in considerazione il bene della conoscenza certa della persona o delle sue qualità essenziali e tantomeno avviene una materiale sostituzione della persona. Ciò che caratterizza la modalità di azione è invece l'utilizzo dei dati ad essa legati, che la identificano "virtualmente" nelle sole operazioni di accesso o di connessione al sistema informatico*».

informatico ad una macchina e quindi al soggetto»[307], condotta eterogenea rispetto all'attribuzione di un falso nome o un falso stato o comunque di una sostituzione della propria all'altrui persona, perché ciò che caratterizza tale condotta è unicamente l'utilizzo dei dati collegati ad una persona, che può consistere anche in un semplice codice alfanumerico, i quali la identificano "virtualmente" nelle sole operazioni di accesso o di connessione al sistema informatico. Senza dimenticare poi che un sistema informatico non è suscettibile di essere indotto in errore[308], elemento costitutivo soltanto del reato di sostituzione di persona. Ad accogliere questa tesi il problema del concorso di reati non si porrebbe neppure, poiché il furto d'identità digitale così inteso non sarebbe mai riconducibile alla fattispecie di sostituzione di persona, ma unicamente alla frode informatica aggravata. Tuttavia, va rammentato che il legislatore non ha specificato in che cosa consista la condotta di "furto d'identità digitale", che tutt'oggi rimane priva di definizione normativa. Se si fa riferimento all'impersonificazione, come asserito in sede parlamentare, le condotte di cui all'art. 640-*ter* co. 3 c.p. e 494 c.p. diventano sostanzialmente sovrapponibili. Tale opinione si pone in continuità con quella giurisprudenza che applica estensivamente l'art. 494 c.p. ritenendo sussistente la sostituzione di persona nella creazione di un *account* di posta elettronica riferibile ad altra persona[309], nell'utilizzo di un *nickname* riconducibile ad altro soggetto o del suo numero di telefono[310]. Dunque, se si ritiene che il furto d'identità digitale coincida con l'impersonificazione, si può sostenere che il concorso tra le due norme sia soltanto apparente, poiché l'"impersonificazione" altrui su *Internet*, condotta sanzionata anche dall'art. 494 c.p., si combina con la commissione di un illecito patrimoniale, elemento aggiuntivo rispetto alla semplice sostituzione di persona *online*. Tesi, peraltro, avvalorata anche dalla giurisprudenza più recente[311]. Per quanto riguarda il bene giuridico tutelato, la giurisprudenza ha qualificato anche la sostituzione di persona come illecito plurioffensivo[312], che non tutela unicamente la pubblica fede, ma anche l'identità personale

[307] CIPOLLA P., *Social network*, cit., p. 2675.
[308] PICOTTI L., *Sistematica dei reati informatici*, cit., p. 31.
[309] V. Cass. pen., sez. III, 15 dicembre 2011, n. 12479.
[310] V. Cass. pen., sez. V, 28 novembre 2012, n.18826.
[311] V. Cass. pen., sez. II, 2 luglio 2020, n. 23760, cit., in motivazione «*Il richiamo contenuto nel ricorso alla nuova fattispecie aggravata di cui all'art. 640 ter c.p., comma 3 va nella direzione opposta alla conclusione cui intende pervenire la difesa, poichè si può ben sostenere che la nuova formulazione - che non a caso ha introdotto una aggravante a effetto speciale - supera la duplicazione della condotta illecita sotto sue concorrenti fattispecie: duplicazione che prima di tale modifica era pertanto del tutto giustificata e coerente col sistema, integrando un concorso formale di reati*».
[312] Così Cass pen., sez. V, 27 marzo 2009, n. 21574, secondo cui «*Il delitto di sostituzione di persona (art. 494 c.p.) ha natura plurioffensiva, essendo preordinato non solo alla tutela di interessi pubblici ma anche di quelli del soggetto privato nella cui sfera giuridica l'atto sia destinato ad incidere concretamente, con la conseguenza che quest'ultimo riveste la qualità di persona offesa dal reato e, in quanto tale, è legittimato a proporre*

del soggetto vittima della falsa impersonificazione, allo stesso modo dell'art. 640-*ter* co. 3 c.p. In ogni caso, anche a non voler accedere alla tesi della specialità, è ipotizzabile un assorbimento del reato di sostituzione di persona nella frode informatica aggravata dal furto o indebito utilizzo dell'identità digitale, che in tal modo assumerebbe la natura di reato complesso[313], tesi che trova conferma considerando i limiti edittali previsti dalle due norme.

Per quanto riguarda specificamente gli attacchi informatici *man-in-the-middle* si pone anche il problema del concorso tra frode informatica e le fattispecie previste in tema di intercettazioni informatiche. Sul punto, la giurisprudenza ha ritenuto che il delitto di cui all'art. 617-*quater* c.p. e quello di frode informatica possano concorrere tra loro, in ragione della diversità dei beni giuridici tutelati e delle condotte sanzionate, dato che la prima fattispecie è diretta a garantire la libertà e la segretezza delle comunicazioni telematiche, mentre la frode informatica contempla l'alterazione dei dati immagazzinati nel sistema al fine della percezione di ingiusto profitto e nasce con la *ratio* di offrire tutela al patrimonio[314]. Effettivamente i due reati si consumano in momenti differenti, per cui non possono essere tra loro in rapporto di specialità e si deve necessariamente concludere per il concorso. Anche in questo caso va però evidenziato che vi è pur sempre l'aggravante di cui all'art. 640-*ter* c.p. del furto o indebito utilizzo di identità digitale. Poiché per "rubare" le credenziali altrui è necessario intercettare i dati sul computer della vittima, le condotte sanzionate vengono a coincidere. Si può, dunque, ritenere che l'art. 640-*ter* co. 3 c.p., proprio perché circostanza aggravante che accede ad una frode informatica, sia speciale rispetto all'art. 617-*quater* c.p. e che si applichi solo la prima delle due fattispecie. Questa può essere considerata anche come reato complesso, dato che l'intercettazione fraudolenta dei dati di accesso al *computer* altrui può considerarsi elemento costitutivo della frode informatica aggravata dal furto d'identità digitale. Alla stessa identica conclusione si può giungere con riferimento al reato di cui all'art. 617-*quinquies* c.p., tesi con cui concorda anche la giurisprudenza della Cassazione, secondo cui il delitto di installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche è assorbito in quello di frode informatica nel caso in cui, installato il dispositivo atto ad intercettare comunicazioni di dati, abbia luogo la captazione. Si evidenzia, infatti, che in questo caso la condotta preparatoria e di pericolo di cui al primo reato si trasforma nell'alterazione del

opposizione alla richiesta di archiviazione». In tal senso anche in dottrina, v. MARRAFFINO M., *La sostituzione di persona mediante furto d'identità digitale*, cit., p. 311.

[313] CAJANI F., *La tutela penale dell'identità digitale*, cit., p. 1097; MINICUCCI, *Le frodi informatiche*, cit., p. 839 s.

[314] Così Cass. pen., sez. V, sentenza 9 ottobre 2020, n. 869.

funzionamento o, comunque, in un intervento illecito sul sistema informatico, coincidendo con le modalità realizzative tipiche della frode informatica[315].

Il problema dell'individuazione dei rapporti tra le diverse norme si pone anche con riferimento ai reati contro il patrimonio, nonché con le fattispecie poste a tutela del patrimonio in senso lato. Si è già evidenziato che la frode informatica e le fattispecie di danneggiamento informatico sono tra loro incompatibili (v. *supra* par. 4). Ma pacificamente va anche escluso che il delitto di frode informatica concorra con la truffa, in quanto le due fattispecie sono in rapporto di specialità reciproca[316].

Più problematico, invece, è il rapporto con la fattispecie di indebito utilizzo di carte di credito. A tal proposito, va evidenziato che le Sezioni Unite hanno escluso il concorso tra quest'ultima fattispecie e il reato di truffa, in quanto tra le due norme vi sarebbe il rapporto di genere a specie di cui all'art 15 c.p.[317]. Non si è in presenza di due fatti completamente distinti, proprio perché l'adozione di artifici o raggiri è uno dei possibili modi in cui si manifesta l'indebito utilizzo di una carta di credito, senza dimenticare che la tutela del patrimonio individuale, che costituisce l'obiettività giuridica della truffa, non è estranea alla *ratio* incriminatrice della fattispecie di indebito utilizzo di carte di credito. In questo caso la Corte ha quindi stabilito che l'indebita utilizzazione, a fine di profitto proprio o altrui da parte di chi non ne sia titolare, di carte di credito o analoghi strumenti di prelievo o pagamento, integra il reato di indebito utilizzo di strumenti di pagamento diversi dai contanti e non quello di truffa, che resta assorbito.

Giurisprudenza più recente si riporta al contenuto di questa pronuncia per escludere il concorso tra l'art 640-*ter* c.p. e l'indebito utilizzo di carta di credito[318]. Ma in seguito è

---

[315] Cass. pen., sez. V, sentenza 7 settembre 2021, n. 42183.

[316] MANTOVANI F., *Dir. pen.*, *PS*, cit., p. 227.

[317] «*Fra la disposizione relativa al delitto di truffa e quella relativa all'indebito utilizzo di carte di credito da parte del non titolare di cui all'art. 12 d.l. 3 maggio 1991 n. 143, conv. in l. 5 luglio 1991 n. 197, deve essere escluso il concorso di reati sia perché non si è in presenza di due fatti completamente distinti dalla materialità della condotta - dal momento che l'adozione di artifici o raggiri è uno dei possibili modi in cui si manifesta l'indebito utilizzo di una carta di credito - sia perché la tutela del patrimonio individuale, che costituisce l'obiettività giuridica della truffa, non è estranea alla "ratio" incriminatrice dell'art. 12; ne consegue che tra le due norme sussiste un rapporto di genere a specie sussumibile all'interno dell'art. 15 c.p., tale per cui la condotta di "indebito utilizzo" di cui all'art. 12 può essere considerata speciale rispetto a quella prevista dall'art. 640 c.p., e dunque unicamente applicabile al fatto concreto*»*:* così Cass. pen. sez. un., 28 marzo 2001, n. 22902.

[318] Cass. pen., sez. II, 10 gennaio 2012, n. 11699 ammette il concorso tra truffa ed indebito utilizzo di carte di credito in base al fatto che «*tale principio* (che esclude il concorso, N.d.R.)*, però, come risulta chiaramente anche dalla motivazione della suddetta sentenza delle Sezioni Unite, riguarda la fattispecie illecita di cui alla prima parte del citato art. 12 (ora confluito nell'art. 55 cit.), che prevede la condotta di "indebita utilizzazione" di carte di credito o di pagamento, non la diversa fattispecie di cui alla seconda parte, che prevede la specifica condotta di "falsificazione o alterazione di carte di credito". Quest'ultima condotta - e non solo quella di indebita utilizzazione - è proprio quella che è stata contestata al P. e che può dar luogo ad una autonoma*

sorto un contrasto giurisprudenziale circa la qualificazione del fatto di colui che utilizza carte di credito clonate[319]. Secondo un primo orientamento giurisprudenziale, la fattispecie applicabile sarebbe unicamente la frode informatica, in quanto l'elemento specializzante consisterebbe nell'utilizzazione "fraudolenta" del sistema informatico, che assorbirebbe la generica indebita utilizzazione di una carta di credito[320]. Tale orientamento trova anche consensi in dottrina, ove si evidenzia che la frode informatica ha quali ulteriori elementi specializzanti la necessità dell'ingiusto profitto con altrui danno[321]. Per un diverso orientamento, invece, integra il reato di indebita utilizzazione di carte di credito e non quello di frode informatica il prelievo di denaro contante presso lo sportello *bancomat* di una banca mediante l'abusivo utilizzo di supporti magnetici con dati clonati, perché non vi sarebbe né l'alterazione del sistema informatico o telematico, né l'abusivo intervento sui dati, ovvero non sarebbero integrati gli elementi costitutivi della frode informatica[322]. Anche tale interpretazione giurisprudenziale incontra il favore di altri autori, che evidenziano come nei casi di utilizzo abusivo di una carta magnetica altrui per prelevare denaro da un bancomat mancherebbe l'esecuzione arbitraria di una successiva operazione economica. In questi casi non possono essere considerati oggetto di "*intervento senza diritto*" i dati relativi alla situazione del conto corrente cui è collegata la carta: i dati in questione vengono modificati in coincidenza con l'abuso effettuato, e l'abuso stesso segna il momento finale del processo di elaborazione, che coincide temporalmente con la fuoriuscita delle banconote dall'apparecchio, per cui difetterebbe in tali situazioni il momento iniziale o intermedio dell'alterazione o dell'indebito utilizzo di dati, elemento costitutivo della frode informatica[323].

A ben guardare, tuttavia, il contrasto presenta un equivoco di fondo, perché di per sé

---

contestazione di reato in concorso con il delitto di truffa, posto che non ogni artificio o raggiro comporta un'attività di falsificazione» La Corte poi riqualificando il fatto in precedenza addebitato all'imputato come truffa in frode informatica, implicitamente ammette il concorso tra l'art *640-ter* c.p. e l'art. 55 d.lgs. cit.

[319] Contrasto giurisprudenziale rilevato anche da Cass. pen., sez. II, 14 febbraio 2017, n. 8913, la quale tuttavia non si pronuncia sul punto in quanto annulla senza rinvio la sentenza impugnata per intervenuta prescrizione.

[320] In tal senso Cass. pen., sez. II, 15 aprile 2011, n. 17748, secondo cui «*integra il delitto di frode informatica, e non quello di indebita utilizzazione di carte di credito, colui che, servendosi di una carta di credito falsificata e di un codice di accesso fraudolentemente captato in precedenza, penetri abusivamente nel sistema informatico bancario ed effettui illecite operazioni di trasferimento fondi, tra cui quella di prelievo di contanti attraverso i servizi di cassa continua*»; in senso conforme anche Cass. pen., sez. II, 13 ottobre 2015, n. 50140, la quale in motivazione ritiene decisiva la sussistenza dell'elemento specializzante, costituito dall'utilizzo "fraudolento" del sistema informatico.

[321] LAZZARI C., *Riciclaggio di carte di credito e truffa: concorso di reati o concorso di norme?*, in *Cass. pen*., 2001, n. 9, p. 2463 ss., p. 2473.

[322] Così Cass. pen., sez. VI, sentenza 14 gennaio 2016, n. 1333.

[323] Cfr. PECORELLA C., *Il diritto penale dell'informatica*, cit., p. 104 s.

la carta di credito clonata non è genuina, ma è contraffatta, dato che imita una carta autentica. Dunque, in tali casi ben può dirsi integrata astrattamente anche la fattispecie di frode informatica, dato che la nozione di "indebito utilizzo" coincide con ogni forma di interferenza in un processo di elaborazione dei dati[324], per cui tale condotta può essere integrata anche mediante l'introduzione nel sistema *bancomat* di dati falsi, quali quelli di una carta di credito contraffatta. Pertanto, sulla falsariga di quanto affermato dalle Sezioni Unite per la truffa, si può ritenere che la frode informatica sia speciale rispetto all'indebito utilizzo di carta di credito, in quanto l'utilizzo di una carta alterata o contraffatta può costituire una modalità di manipolazione o indebito intervento sul sistema informatico.

Resta però il problema del concorso con la fattispecie di falsificazione o alterazione di carte di pagamento di cui alla seconda parte dell'art. 493-*ter* c.p., dato che, come sopra evidenziato, la carta clonata è una carta falsificata, e tale condotta ben può integrare anche la diversa fattispecie di falsificazione o alterazione di carte di credito, la quale, non essendo in rapporto di specialità con la frode informatica, astrattamente potrebbe con essa concorrere.

Come già evidenziato (v. *supra*, par. 3), il problema dei rapporti tra le due norme si è ulteriormente aggravato con l'ampliamento dell'oggetto del reato della fattispecie di cui all'art. 493-*ter* c.p. ad opera del d.lgs. 184/2021. I primi commentatori hanno proposto di ritenere applicabile l'art. 493-ter c.p. a tutte le ipotesi di utilizzo illegittimo di mezzi di pagamento immateriali e di considerare come residuale l'art. 640-*ter* c.p., nell'ipotesi aggravata di nuova introduzione[325]. Tuttavia, tale soluzione non è condivisibile, perché finirebbe per abrogare tacitamente la fattispecie di frode informatica. Infatti, per la stessa struttura della fattispecie, che richiede l'alterazione o l'intervento senza diritto su un sistema informatico, appare difficile ipotizzare la commissione di frodi informatiche attraverso strumenti che non siano proprio quelli di pagamento diversi dai contanti. Senza poi contare che soltanto la fattispecie di frode informatica prevede la circostanza aggravante del fatto commesso con furto o indebito utilizzo dell'identità digitale. La frode informatica, ai fini della sua integrazione, richiede l'effettivo conseguimento di un ingiusto profitto con altrui danno, per cui nell'ipotesi di clonazione e successivo indebito uso di uno strumento di pagamento si potrebbe ritenere che la frode informatica aggravata sia idonea a sanzionare il fatto considerato nel suo intero disvalore, ricomprendendo sia la falsificazione o

[324] AMATO D., *Sub Art. 640-ter,* cit., p. 2280.
[325] In tal senso BERNARDONI P., *Attuazione degli obblighi europei in materia di lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti: prima lettura del d.lgs. n. 184 del 2021*, in *Sist. pen.*, 3 febbraio 2021.

l'alterazione, sia il suo successivo utilizzo al fine di sottrarre indebitamente il denaro altrui[326]. Inoltre, dato che il reo sfrutta le credenziali della vittima fingendosi quest'ultima per effettuare operazioni non autorizzate, tale condotta può essere ricompresa nella nozione di «*indebito utilizzo dell'identità digitale*» di cui al co. 3 dell'art. 640-*ter* c.p. Per questo motivo, si può ritenere che nei casi in cui si sia verificato l'effettivo depauperamento della vittima, l'indebito utilizzo, la falsificazione o l'alterazione dello strumento di pagamento possano considerarsi assorbite nel più grave reato di frode informatica aggravata di cui all'art. 640-*ter* co. 2 e 3 c.p.

Infine, anche per il reato di cui all'art. 493-*ter* c.p. si propone il problema dell'individuazione dei rapporti con l'art. 494 c.p. Quando, infatti, il reo indebitamente utilizza la carta di credito altrui si "sostituisce" al legittimo titolare della carta, condotta che astrattamente può integrare entrambe le fattispecie. A tal proposito, la giurisprudenza ritiene che il delitto di indebita utilizzazione di carta di credito assorba quello di cui all'art. 494 c.p. nel caso in cui la sostituzione sia attuata con la stessa condotta materiale integrante il primo reato, poiché l'ipotesi delittuosa di cui all'art. 493-*ter* c.p. lede, oltre al patrimonio, anche la pubblica fede, mentre l'art. 494 c.p. contiene una clausola di riserva destinata ad operare anche al di là del principio di specialità[327]. Anche in questo caso, dunque, ai fini dell'esclusione del concorso di reati la giurisprudenza utilizza un criterio diverso da quello della specialità. In questo caso, dato il trattamento sanzionatorio molto più elevato stabilito per l'art. 493-*ter* c.p., è ben possibile ritenere che quest'ultimo reato assorba integralmente il disvalore della sostituzione di persona.

6. Il concorso di persone nel reato

Le fattispecie esaminate pongono problemi anche con riferimento alla configurabilità del concorso di persone. Come evidenziato, infatti, è sempre più raro che colui che si appropria direttamente del denaro dal sistema di *home banking* della vittima o attivi un *ransomware* in grado di bloccare il computer di un'azienda sia la stessa persona che si è illecitamente appropriata delle credenziali del correntista o comunque abbia progettato il *malware* in grado di bloccare il sistema informatico. Si pone, dunque, il problema della configurabilità del concorso di persone nei reati contro il patrimonio in senso lato da parte di coloro che hanno fornito un effettivo aiuto a colui che ha poi materialmente portato a

[326] In tal senso anche PICOTTI L., *Sistematica*, cit., p. 57.
[327] Cass. pen. sez. II, sentenza 22 settembre 2021, n. 39276.

compimento l'attacco informatico.

Nel codice penale italiano esiste un modello unitario di concorso, che considera rilevante qualsiasi apporto dato alla realizzazione del reato, non essendovi una tipizzazione dei diversi possibili contributi concorsuali con predeterminazione delle cornici edittali in base alla loro rilevanza. Il dosaggio delle pene non è legato ad un sistema chiuso di figure definite, ma ad un criterio elastico, ovvero l'importanza del contributo, che diviene criterio d'individualizzazione della pena[328].

In tale contesto, l'art. 110 c.p. ha funzione integrativa, per cui talune azioni restano atipiche perché rappresentano uno stadio preliminare dell'offesa, ma accostate al fatto tipico commesso da altri, che aiutano a realizzare, acquistano un sicuro rilievo penale[329]. Dunque, accanto alla fattispecie tipica nasce la fattispecie eventualmente plurisoggettiva, autonoma e dotata di una sua tipicità, a forma libera e causalmente orientata, che rende rilevante ogni condotta atipica dotata di rilevanza eziologica rispetto alla commissione della fattispecie di parte speciale.

La fattispecie plurisoggettiva di cui all'art. 110 c.p. è caratterizzata da diversi requisiti, ovvero la pluralità di concorrenti, la realizzazione di un fatto materiale di reato e il contributo di ciascun concorrente alla sua realizzazione, oltre al dolo di partecipazione[330]. Per la definizione dei requisiti minimi della condotta di contributo concorsuale, sono stati proposti in dottrina tre differenti modelli, ovvero il criterio causal-condizionalistico, secondo cui può assumere rilevanza esclusivamente l'azione del partecipe che costituisca *condicio sine qua non* del fatto punibile secondo un giudizio *ex post*, il criterio della prognosi postuma, secondo cui è sufficiente che la condotta del partecipe sia ex ante idonea a facilitare la realizzazione del reato, anche se *ex post* si riveli inutile o persino dannosa, e, infine, il criterio della causalità agevolatrice (o di rinforzo), che afferma la rilevanza, ai fini del concorso, non soltanto del contributo necessario, ma anche di quello che abbia soltanto facilitato la realizzazione del reato, rendendolo più probabile, più facile o più grave, sempre alla stregua di un giudizio *ex post*[331].

Quest'ultimo criterio è quello che viene applicato dalla prevalente giurisprudenza, la quale sostiene che il contributo concorsuale assume rilevanza non solo quando abbia

[328] PEDRAZZI C., *Il concorso di persone nel reato*, Palermo, 1952, ora anche in PEDRAZZI C., *Scritti di diritto penale*. *Vol. I scritti di parte generale*, Milano, 2003, p. 3 ss., p. 136.
[329] *Ibid*., p. 9 s.
[330] Per tutti v. MANTOVANI F., *Diritto penale. PG*, cit., p. 558 ss.
[331] INSOLERA G., voce *Concorso di persone nel reato*, in *Dig. disc. pen.*, vol. II, Torino, 1988, p. 437 ss., p. 458 ss.

efficacia causale, ponendosi come condizione dell'evento lesivo, ma anche quando assuma la forma di un contributo agevolatore, e cioè quando il reato, senza la condotta di agevolazione, sarebbe ugualmente commesso ma con maggiori incertezze di riuscita o difficoltà. Pertanto, è sufficiente che la condotta di partecipazione si manifesti in un comportamento esteriore che arrechi un contributo apprezzabile alla commissione del reato, mediante il rafforzamento del proposito criminoso o l'agevolazione dell'opera degli altri concorrenti e che il partecipe, per effetto della sua condotta, idonea a facilitarne l'esecuzione, abbia aumentato la possibilità di realizzazione del reato, perché in forza del rapporto associativo diventano sue anche le condotte degli altri concorrenti[332].

Con riferimento ai fenomeni criminosi descritti, appare palese che la condotta di colui che vende numeri di carte di credito altrui nel *darkweb* o reti *bootnet* in grado di compromettere il funzionamento di un sistema informatico dia un contributo apprezzabile alla commissione del reato di frode informatica o di danneggiamento informatico, ecc. Anzi, in qualche caso si tratta di un contributo indispensabile, dato che colui che poi effettivamente penetra nel sistema informatico, utilizza le credenziali altrui ecc. non possiede le capacità tecniche per svolgere in autonomia un simile compito. Per fare un paragone con il mondo reale, tale condotta è assimilabile a quella di colui che procura al ladro una chiave falsa dell'appartamento della vittima, in modo che quest'ultimo possa entrarvi e rubare quel che desidera. Sotto questo profilo, dunque, non appaiono esservi ostacoli per l'ammissibilità del concorso di persone.

Serve però il dolo di partecipazione: rappresentazione e volontà del fatto di reato e rappresentazione e volontà di concorrere con altri nella commissione del reato. Il profilo soggettivo, dunque, consiste nella consapevolezza di cooperare[333]. Anche qui in linea teorica non vi sono ostacoli nel ritenere sussistente nelle condotte descritte il dolo di partecipazione, che in molti casi si può desumere dalla stessa natura dei beni compravenduti: la consegna di *password* o credenziali altrui, nonché numeri di carte di credito o *bootnet* di vario tipo viene palesemente effettuata allo scopo di consentire ad altri di commettere un reato informatico quale ad esempio una frode informatica. Anche in questo caso, però, dato che come detto alcuni *software* possono svolgere anche funzioni lecite, è bene valutare sempre in concreto le circostanze, in modo da evitare inammissibili presunzioni di colpevolezza sulla base della

[332] V. *ex multis* Cass. pen., sez. V, sentenza 24 ottobre 2019, n. 43569; Cass. pen., sez. VI, sentenza 28 aprile 2017, n. 36739; Cass. pen., sez. III, sentenza 10 gennaio 2017, n. 29219; Cass. pen., sez. VI, sentenza 13 maggio 2014, n. 36125; Cass. pen., sez. VI, sentenza 25 settembre 2012, n. 36818.
[333] INSOLERA G., *voce Concorso di persone nel reato*, cit., p. 474.

mera natura dell'oggetto.

Si può ritenere, dunque, che lo scambio di oggetti e servizi illegali e/o di provenienza illecita in *Internet* possa essere punito a titolo di concorso di persone nel reato successivamente commesso. Si pone, però, il problema del concorso di reati, dato che molte delle condotte descritte sono già punite da altre norme: basti pensare all'art. 615-*quater* c.p., che sanziona proprio colui che "mette in altro modo a disposizione di altri" gli strumenti del reato. In questo caso, il problema andrà risolto secondo i criteri descritti in precedenza.

7. Considerazioni di sintesi

Dall'analisi appena svolta è possibile concludere che le fattispecie che tutelano direttamente o indirettamente il patrimonio dalle nuove minacce informatiche e cibernetiche sono piuttosto numerose. Emerge, però, come già evidenziato, un'insoddisfazione di fondo per quanto riguarda la tradizionale fattispecie di truffa, il cui trattamento sanzionatorio è inadeguato con riferimento alle truffe realizzate sul *web*, dato che la circostanza aggravante della minorata difesa viene riconosciuta nella quasi totalità dei casi, finendo per diventare l'ipotesi ordinaria di reato.

Inoltre, va evidenziato che la distinzione tra la frode informatica e la falsificazione e l'indebito utilizzo di strumenti di pagamento diversi dai contanti, in particolare con riferimento ai nuovi strumenti immateriali, quali ad esempio le App di *home banking* per *smartphone*, è tutt'altro che ben definita. Ne consegue che la regolazione dei rapporti tra le fattispecie menzionate, caratterizzate da un trattamento sanzionatorio assai differente, è estremamente controversa.

Costituisce un problema generale la definizione dei corretti rapporti tra le diverse fattispecie. Anche questo settore, infatti, esattamente come già osservato per i reati contro la riservatezza informatica, si caratterizza per una sovrabbondanza di norme non coordinate tra di loro e/o eccessivamente ridondanti, con un lungo elenco di condotte con significato simile se non identico. Paradigmatica è la frode informatica, in cui i rapporti tra alterazione e intervento senza diritto sono tuttora poco chiari. Altrettanto per le diverse fattispecie di danneggiamento informatico. La sanzione delle stesse condotte da parte di molteplici fattispecie, nonché lo scarsissimo utilizzo di clausole di sussidiarietà, hanno quale conseguenza la sovrapposizione tra le diverse norme. Infatti, a meno di riconoscere la natura di reato complesso alla frode informatica aggravata o pluriaggravata, seguendo il criterio della specialità di deve necessariamente ritenere che fattispecie quali frode informatica e indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti concorrano

necessariamente tra loro, nonché coi reati posti a tutela della riservatezza informatica, comprese le intercettazioni informatiche. Questo, però, comporta una notevole moltiplicazione delle sanzioni.

Ma l'analisi non può certo limitarsi a questi reati. Infatti, una volta ottenuto il profitto da parte della vittima, si pone il problema di come occultare l'illecita provenienza del denaro, o delle criptovalute, illecitamente ottenuti. Nel prossimo capitolo, dunque, si esaminerà il fenomeno del reimpiego dei capitali illecitamente ottenuti tramite attacchi informatici.

Capitolo IV

Le diverse forme di reimpiego del denaro e dei valori provento dei reati cibernetici

Sommario: 1. Dal riciclaggio al *cyberlaundering*: le molteplici possibilità di reimpiego di denaro offerte dal *web*. - 2. Il quadro normativo europeo: le direttive antiriciclaggio e la prima Direttiva 2018/1673/UE sulla lotta al riciclaggio mediante il diritto penale. - 3. Le fattispecie in materia di riciclaggio presenti nel codice penale. - 3.1. Il riciclaggio ex art. 648-*bis* c.p. - 3.2. Impiego di denaro, beni o utilità di provenienza illecita. – 3.3 L'autoriciclaggio. – 3.4. Le fattispecie di cui all'art. 55 d.lgs. 231/2007. - 4. Il ruolo dei c.d. *financial managers*. - 5. Considerazioni di sintesi.

1. Dal riciclaggio al *cyberlaundering*: le molteplici possibilità di reimpiego di denaro offerte dal *web*

Una volta concluso il *phishing attack* o comunque l'attacco informatico diretto contro il patrimonio, sia esso un *ransomware* o una *advance fee fraud*, per il criminale informatico sorge il problema di nascondere l'illecita provenienza dei proventi. A tal proposito, va evidenziato che tale ultimo stadio è il più rischioso per il criminale, perché il trasferimento dei proventi illeciti dall'ambiente digitale al mondo reale può essere fonte di grosse perdite e, soprattutto, esporre l'autore del fatto al rischio di essere individuato dalle forze dell'ordine[1]. Il criminale informatico, dunque, deve ricorrere all'utilizzo delle tecniche di riciclaggio del denaro, al fine di camuffarne l'origine. In tale contesto assume sempre più rilevanza il ruolo dei *financial managers*, ovvero coloro che, senza essere concorsi nel reato presupposto, nella piena consapevolezza della provenienza illecita o, comunque, accettandone il rischio, a fronte della prospettazione di facili guadagni come compenso della semplice attività richiesta, a seguito di proposte di collaborazione in *Internet*, tramite *e-mail*, contatti in *chat* o messaggi su pagine *web*, ricevono e successivamente trasferiscono le somme di denaro provenienti da delitti commessi dal *phisher*[2]. L'utilizzo del *darkweb*, poi, consente di far perdere più facilmente le tracce del denaro, perché in tale luogo virtuale è possibile ingaggiare *broker* e intermediari finanziari per effettuare una serie di trasferimenti illegali di denaro volti a mascherarne l'origine. Se a ciò si aggiunge lo pseudoanonimato delle valute virtuali, nonché la possibilità di utilizzare i servizi offerti dai c.d. *mixer* o *tumbler*

[1] KOCHHEIM D., *Cybercrime und Strafrecht,* cit., p. 157.
[2] FLOR R., *Phishing e profili penali dell'attività illecita di "intermediazione" del cd. financial manager,* in *Dir. pen. proc.*, 2012, n. 1, p. 55 ss.

per ovviare al problema della tracciabilità della tecnologia *blockchain* appare evidente come le nuove tecnologie costituiscano un potente strumento per riciclare il denaro provento di un attacco informatico contro il patrimonio[3].

Il riciclaggio può essere definito come l'occultamento dell'origine di fondi e beni derivanti dalla commissione di reati, nonché l'infiltrazione di tali fondi e beni nel circuito finanziario ed economico legale[4]. Si tratta di un fenomeno globale e da sempre e in tutto il mondo si incontrano difficoltà nella predisposizione di una regolamentazione normativa del riciclaggio. Questo perché il fenomeno criminoso è estremamente complesso e in costante mutamento, in risposta alle differenti condizioni del mercato e agli interventi di controllo adottati dal legislatore[5]. Inoltre, rappresenta una forma di criminalità che spesso si confonde o sovrappone ad attività economiche del tutto lecite[6].

Il contrasto al riciclaggio si è progressivamente emancipato dal narcotraffico e da altri fenomeni "emergenziali" per legarsi alla tutela di interessi economici[7]. Si è, infatti, preso atto che il fenomeno dell'ingresso dei capitali illeciti coinvolge molteplici settori, con conseguenti gravi effetti sul sistema economico legale. Infatti, esso lede il principio della libera concorrenza, dato che alcuni operatori possono finanziarsi senza fare ricorso al credito bancario o a normali canali legali di finanziamento[8]. Addirittura, è stato definito come «*un fenomeno criminale di dimensioni tali da poter mettere in discussione non solo l'ordine economico del Paese, ma lo stesso ordine democratico*»[9]. Ad essere lesivo, però, non è tanto l'atto di riciclaggio in sé, quanto piuttosto il fatto che tale meccanismo consente ai criminali di godere liberamente dei proventi delle proprie attività illecite[10].

Nella letteratura il fenomeno del riciclaggio viene ricostruito secondo modelli talvolta diversi, grossomodo distinti in "modelli a fasi", "modelli a ciclo" e "modelli a scopo". Nel primo tradizionalmente si suddividono le operazioni finanziarie di riciclaggio in tre fasi[11]. La prima è quella del *placement* o collocamento materiale dei proventi da reato,

---

[3] LEWIS J., *Economic Impact of Cybercrime*, cit., p. 5.
[4] QUEDENFELD R., *Handbuch Bekämpfung der Geldwäsche und Wirtschaftskriminalität*, 2017, Berlin, p. 21
[5] ZANCHETTI M., *Il riciclaggio di denaro proveniente da reato*, Milano, 1997, p. 6.
[6] MANES V., *Il riciclaggio dei proventi illeciti: teoria e prassi dell'intervento penale*, in *Riv. trim. dir. pen. econ.*, 2004, n. 1-2, p. 35 ss., p. 36.
[7] DELL'OSSO A.M., *Riciclaggio Di Proventi Illeciti e Sistema Penale*, Torino, 2017, p. 20.
[8] AMATO G., *Il riciclaggio del denaro "sporco". La repressione penale dei profitti delle attività illecite*, Roma, 1993, p. 18 s.
[9] MOCCIA S., *Effettività e normativa antiriciclaggio*, in E. Palombi (a cura di), *Il riciclaggio dei proventi illeciti. Tra politica criminale e diritto vigente*, Napoli, 1996, p. 303 ss., p. 305.
[10] SAXENA R., *Cyberlaundering: The Next Step for Money Launderers*, in *St. Thomas L. Rev.*, 1998, vol. 10, n. 3, p. 685 ss., p. 686 s.
[11] MAITLAND IRWIN A.S., RAYMOND CHOO K., LIU L., *An analysis of money laundering and terrorism financing typologies*, in *Journal of Money Laundering Control*, 2012, vol. 15, n. 1, p. 85 ss., p. 94 ss.

normalmente denaro contante, attraverso una serie di operazioni quali deposito, cambio, trasferimento, acquisto di beni, ecc. In tale fase, dunque, si effettua la raccolta di una certa somma di denaro o di una certa quantità di valori provenienti da reato, che poi vengono collocati presso istituzioni o intermediari finanziari tradizionali e non, direttamente nel mercato con l'acquisto di beni o fuori dal Paese. Questa è la fase nella quale è più facile l'individuazione della natura illecita dei proventi, motivo per cui la c.d. normativa preventiva antiriciclaggio ha ad oggetto proprio questa fase[12]. La seconda fase del *layering*, o stratificazione, implica il compimento di ulteriori operazioni, di natura perlopiù finanziaria, volte a separare i proventi illeciti dalla loro fonte, in modo da rendere più difficile l'individuazione della provenienza delittuosa del bene. Si evidenzia che in questa fase la gestione delle operazioni è spesso affidata ad intermediari esterni, che svolgono lo specifico compito di prendere in carico i capitali appena inseriti nei mercati legali e restituirli all'esito delle operazioni[13]. Infine, l'ultima fase di *integration*, o integrazione, implica l'integrazione dei proventi illeciti con le ricchezze di provenienza lecita. Se le operazioni precedenti hanno avuto successo si reimmettono i proventi nel circuito economico legale facendo in modo che il loro ingresso appaia frutto di un'operazione finanziaria ordinaria, con fondi di provenienza pienamente legittima[14].

Lo schema trifasico rappresenta senz'altro un modello valido per l'individuazione dei momenti necessari per completare il percorso d'infiltrazione dei capitali illeciti nell'economia legale[15]. Tuttavia, si rivela troppo rigido. Si evidenzia, infatti, che spesso le tre fasi non sono che condotte tra loro isolate, che non necessariamente costituiscono riciclaggio, dato che con le stesse non si occulta l'origine dei beni che, invece, vengono unicamente trasferiti o trasformati[16]. Per questo motivo, sono stati proposti altri modelli volti a superare la rigidità di tale primo schema, ovvero i modelli a scopo o a ciclo, che evidenziano come il processo di riciclaggio consista in realtà nella fusione delle diverse fasi, ovvero il ciclo, orientate ad un fine preciso. In ogni caso tutti i modelli evidenziano che il riciclaggio è un fenomeno complesso, che difficilmente si riduce ad un'unica operazione[17].

Lo sviluppo e la diffusione delle nuove tecnologie nonché la possibilità di gestire rapporti bancari via *web,* rendono più semplice realizzare operazioni di riciclaggio del

[12] DELL'OSSO A.M., *Riciclaggio Di Proventi Illeciti,* cit., p. 35.
[13] *Ibid*., p. 41.
[14] ZANCHETTI M., *Il riciclaggio di denaro*, cit., p. 10 ss.
[15] LEVI M., REUTER P., *Money Laundering*, in *Crime & Just*., 2006, n. 34, p. 289 ss., p. 311.
[16] PRIETO DEL PINO A.M., GARCÍA MAGNA D.I., MARTÍN PARDO A., *La deconstrucción del concepto de blanqueo de capitales*, in *InDret*, 2010, n. 3, p. 1 ss., p. 5.
[17] ZANCHETTI M., *Il riciclaggio di denaro*, cit., p. 17.

denaro. Oggi è possibile effettuare operazioni di *layering* o *integration* senza alcun contatto materiale col denaro o coi valori oggetto dell'operazione stessa, talvolta persino senza che gli stessi cambino di mano. La maggior parte delle banche, infatti, offre la possibilità di effettuare quasi tutte le operazioni bancarie standard via Internet. In questo modo è possibile creare e controllare un numero illimitato di conti senza attirare l'attenzione degli istituti finanziari in cui sono stati aperti. In questi conti vengono effettuati depositi multipli di somme moderate di denaro provento di reato, sempre al di sotto della soglia di allerta per le operazioni sospette nei diversi Stati, il cui importo complessivo potrebbe essere molto elevato, nel tentativo di eludere i controlli[18]. Attraverso i sistemi di *home banking*, dunque, è molto agevole muovere modeste, ma molteplici, somme di denaro da un Paese ad un altro in pochi minuti. Il fenomeno del c.d. *cyberlaundering*, dunque, assume sempre più rilevanza, per non parlare poi dei sistemi alternativi quali *Westunion*.

Il *cyberlaundering* può essere definito come una nuova forma di riciclaggio, che sfrutta il *web* e le nuove tecnologie[19]. Esso non rappresenta un'alternativa al riciclaggio tradizionale, ma indica l'utilizzo delle nuove tecnologie e dei moderni sistemi di pagamento per riciclare il denaro[20]. Questi ultimi, infatti, consentono di risolvere uno dei più grandi problemi delle operazioni di riciclaggio di denaro, ovvero la movimentazione fisica di grosse somme di denaro, con conseguenti rischi di individuazione[21]. Alcuni autori distinguono tra due forme di *cyberlaundering*, ovvero il riciclaggio digitale strumentale e il riciclaggio digitale integrale[22]. Nel primo caso il denaro non è *ex ante* dematerializzato, per cui è ancora richiesta una movimentazione del denaro contante, che dev'essere trasformato in moneta elettronica[23]. Per questo motivo, può essere definito come *cyberlaundering* "parziale"[24]. Viceversa, nel riciclaggio digitale integrale le somme di denaro da riciclare sono già disponibili in forma dematerializzata.

---

[18] PRIETO DEL PINO A.M., GARCÍA MAGNA D.I., MARTÍN PARDO A., *La deconstrucción del concepto de blanqueo de capitales*, cit., p. 16.
[19] PICOTTI L., *Profili penali del cyberlaundering: le nuove tecniche di riciclaggio*, in *Riv. trim. dir. pen. econ*., 2018, n. 3- 4, p. 590 ss., p. 591.
[20] SAXENA R., *Cyberlaundering*, cit., p. 706 s.; DELL'OSSO A.M., *Riciclaggio Di Proventi Illeciti*, cit., p. 36.
[21] SIMONCINI E., *Il Cyberlaundering: la «nuova frontiera» del riciclaggio*, in *Riv. trim. dir. pen. econ*., 2015, n. 4, p. 897 ss., p. 899.
[22] CROCE M., *Cyberlaundering e valute virtuali. La lotta al riciclaggio nell`era della distributed economy*, in *Sist. Pen.*, 2021, n. 4, s. 127 ff., s.; SICIGNANO G.J., *Money Laundering Using Cryptocurreny*, in *Athens Journal of Law*, n. 7, s. 253 ff., s. 259.
[23] SIMONCINI E., *Il Cyberlaundering*, cit., p. 900.
[24] CROCE M., *Cyberlaundering e valute virtuali*, cit., p. 136.

Anche il *cyberlaundering* fa parte del più vasto fenomeno del *cybercrime*, diffuso a livello globale. Può infatti accadere che le somme di denaro illecitamente ottenute vengano impiegate in uno Stato diverso rispetto a quello nel quale le stesse sono state ottenute[25], situazione, questa, che, come si esaminerà nel prosieguo, è stata espressamente presa in considerazione dai legislatori tedesco e spagnolo nelle rispettive fattispecie che sanzionano il riciclaggio di denaro. Come già evidenziato, infatti, attraverso i sistemi di *e-banking* è agevole manovrare numerosi conti correnti aperti in diversi istituti anche in territori molto lontani tra loro. A tale scopo le attività di *Money Transfer* svolgono un ruolo centrale, dato che in numerosi Paesi di destinazione delle risorse i capitali trasferiti non sono soggetti ad alcuna vigilanza[26].

Sempre più spesso il provento del reato è costituito dalle criptovalute, in particolare *Bitcoin*[27]. Questo perché molte volte i criminali informatici richiedono che il pagamento del riscatto a seguito dell'installazione di un *ransomware* avvenga in criptovalute.

Le valute virtuali quali *Bitcoin*, *Monero* o *ZCash*, che garantiscono ai loro utenti lo pseudonimato o addirittura l'anonimato, svolgono un ruolo importante nel *phishing* e si prestano bene al riciclaggio di denaro. Esse, infatti, combinano la possibilità di effettuare transazioni transfrontaliere di moneta elettronica con l'anonimato caratteristico del contante e pertanto svolgono un ruolo importante nelle operazioni di riciclaggio di denaro. Anche se l'anonimato delle criptovalute è variabile a seconda della loro tipologia, dato che alcune sono completamente anonime, mentre in altri casi è possibile visionare le transazioni[28], gli ostacoli pratici per le Autorità pubbliche nel determinare la reale identità del proprietario del *wallet* o delle criptovalute sono ancora troppo elevati[29]. In ogni caso, nella maggior parte dei casi i criminali non solo trasferiscono i proventi del reato all'interno di una *blockchain*, ma sfruttano anche l'opportunità di modificare quest'ultima. Infatti, spesso vengono utilizzati i servizi offerti dai c.d. *tumbler* per rendere più difficile il tracciamento delle transazioni[30]. Trattasi di servizi di anonimizzazione, che possono essere utilizzati per la compromissione

[25] NILSSON H.G., *The Council of Europe Laundering Convention: A Recent Example of a Developing International Criminal Law*, in *Crim. L. Forum*, 1991, vol. 2, n. 3, p. 419 ss., p. 425.
[26] LAUDATI A., *Terrorismo internazionale, criminalità organizzata e Money Transfer*, in *Per aspera ad veritatem*, 2002, n. 24, p. 25 ss.
[27] VAN WEGBERG R., OERLEMANS J., VAN DEVENTER O., *Bitcoin money laundering: mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin*, in *J. Financ. Crime*, 2018, vol. 25, n. 2, p. 419 ss., p. 421.
[28] TROPINA T., *Fighting money laundering in the age of online banking, virtual currencies and internet gambling*, in *ERA Forum*, 2014, n. 15, p. 69 ss., p. 76.
[29] BUSSMAN K.D., *Geldwäscheprävention im Markt - Funktionen, Chancen und Defizite*, 2018, Berlin, s. 138; PLANTAMURA V., *Il Cybericiclaggio*, s. 881.
[30] MAUME P., MAUTE L., FROMBERGER M., *Rechtshandbuch Kryptowerte*, cit., p. 533.

della catena *blockchain*, in modo da non rendere individuabili i trasferimenti effettuati. I *tumbler* o *mixer* mescolano e scambiano automaticamente i *Bitcoin* di diversi utenti e li trasferiscono a nuovi indirizzi precedentemente definiti. A tale scopo, il *tumbler* mantiene numerose chiavi pubbliche e trasferisce le criptovalute dai suoi clienti in modo casuale e automatico tra di loro. I *Bitcoin* vengono quindi scambiati con i *bitcoin* di altri utenti, divisi tra più indirizzi di destinazione e trasferiti a intervalli casuali, in questo modo compromettendo la catena *blockchain* (sul punto v. *supra*, cap. I, par. 4.4).

Peraltro, poiché basate su un sistema *peer-to-peer*, le criptovalute consentono di effettuare facilmente e rapidamente trasferimenti di valori monetari senza la necessità di utilizzare gli istituti di credito o altri intermediari che adottano disposizioni di segnalazione e/o identificazione della clientela volte ad ostacolare il riciclaggio di denaro[31]. Va infatti evidenziato che, a prescindere dalle opinioni espresse dalla dottrina in merito alla qualificazione giuridica delle criptovalute, alle transazioni relative alle stesse non si applica la normativa europea in materia di servizi di pagamento, dato che la direttiva 2015/2366/UE o Payment Services Directive 2 (c.d. PSD2), recepita nel nostro ordinamento col d.lgs. 15 dicembre 2017, n. 218, precisa che il suo ambito applicativo è ristretto ai soli pagamenti denominati in moneta legale[32]. Tale normativa, infatti, prevede obblighi di trasparenza e sicurezza nei confronti dei prestatori dei servizi di pagamento che, invece, nell'ambito delle transazioni in criptovalute non sono stabiliti. Inoltre, le criptovalute non sono soggette in tutte le parti del mondo alla normativa antiriciclaggio, il che le rende uno strumento adatto per l'occultamento e il reimpiego di capitali illeciti[33].

I meccanismi del *cyberlaundering* sono gli stessi del riciclaggio tradizionale[34]. Anche in questo caso, infatti, possono distinguersi diverse fasi[35]. Tuttavia, gli strumenti di pagamento *online* rendono superfluo il compimento di operazioni di *placement*, dato che il denaro provento di reato è già presente *online*, mentre nel caso delle valute virtuali il denaro è già stato "depositato" all'interno di una sorta di istituto finanziario non regolamentato[36].

Le possibilità offerte dal *web* per il riciclaggio non riguardano unicamente le criptovalute. Costituiscono ottimi strumenti anche le scommesse illegali ed i giochi

[31] SAXEBA R., *Cyberlaundering*, cit., p. 688.
[32] V. artt. 2 e 3 direttiva 2015/2366/UE cit. Per approfondire v. MASI D., *Le criptoattività*, cit., p. 253.
[33] TROPINA T., *Fighting money laundering in the age of online* banking, cit., p. 75.
[34] SAXEBA R., *Cyberlaundering*, cit., p. 707.
[35] PICOTTI L., *Profili penali del cyberlaundering*, cit., p. 592.
[36] TROPINA T., *Fighting money laundering in the age of online banking*, cit., p. 71; FILIPKOWSKY W., *Cyber Laundering: An Analysis of Typology and Techniques*, in *Int. J. Crim. Justice Sci*., 2008, vol. 1, n. 3, p. 15 ss., p. 20.

d'azzardo in rete, oggi estremamente diffusi e di immediata fruibilità. Inoltre, sia nel *dark web* che nel *web* vengono offerti "sevizi finanziari" per effettuare passaggi di denaro e transazioni strumentali via *web*, in modo da rendere impossibile o molto difficile risalire alla loro origine o all'identità dei soggetti da cui realmente provengano o a cui siano destinati. Tali offerte includono l'acquisto di valori mobiliari o di immobili ovvero reinvestimenti di ogni tipologia in tempi brevissimi, nella maggior parte situati in paesi o continenti diversi da quelli d'origine, preferibilmente in paradisi fiscali, in modo da occultare o comunque da far perdere subito le tracce, con una serie adeguata di movimentazioni o transazioni elettroniche, della provenienza (soggettiva od oggettiva) dei capitali, dei valori, delle "utilità", che in questo modo vengono ripuliti[37].

Ciò premesso, va ora analizzata la specifica rilevanza giuridico-penale dell'insieme di comportamenti sopra descritti. In particolare, si deve esaminare se ed eventualmente quali fattispecie presenti nel nostro ordinamento in materia di riciclaggio possano ricomprendere le diverse possibili fasi del complesso fenomeno del *cyberlaundering*. Va però evidenziato che nell'ambito del riciclaggio a venire ad evidenza non sono unicamente le fattispecie penali, ma anche una disciplina normativa caratterizzata da una serie di disposizioni relative alla prevenzione del riciclaggio di denaro di provenienza illecita, di derivazione sovranazionale. Come si esaminerà nel paragrafo successivo, infatti, la cornice normativa internazionale in materia di antiriciclaggio è costituita da un'articolazione di fonti rappresentata da standard internazionali, norme europee e convenzioni internazionali volti proprio ad individuare questi obblighi di identificazione nonché i soggetti obbligati.

2. Il quadro normativo europeo: le direttive antiriciclaggio e la prima Direttiva 2018/1673/UE sulla lotta al riciclaggio mediante il diritto penale

Una volta compresa la natura transnazionale del fenomeno del riciclaggio, la comunità internazionale iniziò ad adottare una serie di iniziative finalizzate ad assicurarne una repressione articolata e realmente incisiva. Sin dalle prime iniziative si prese atto che il sistema bancario non solo può svolgere un ruolo preventivo estremamente efficace, ma la sua collaborazione con le autorità giudiziarie e di polizia può costituire un significativo aiuto nello scoprire un fatto di trasferimento e riciclaggio dei capitali di provenienza illecita. Pertanto, sin dagli anni '80 i documenti e i provvedimenti sovranazionali più significativi in materia hanno evidenziato la necessità che le istituzioni finanziarie assumessero obblighi

[37] PICOTTI L., *Profili penali del cyberlaundering*, cit., p. 594.

antiriciclaggio quali l'identificazione della clientela e la segnalazione delle operazioni sospette[38].

Decisivo è stato l'impulso proveniente dal Governo americano, il quale iniziò a guardare al riciclaggio come vero bersaglio della lotta al narcotraffico e nel 1986 adottò il *Money laundering Control Act*. Dopodiché gli Stati Uniti sfruttarono la propria posizione nelle sedi internazionali per spingere verso l'adozione di modelli comuni in ambito internazionale[39]. L'esempio americano, dunque, ha notevolmente influenzato la stesura delle fattispecie penali di riciclaggio in numerosi ordinamenti, anche europei, ed è stato determinante nella redazione di alcuni atti internazionali, a partire dalla Convenzione ONU contro il traffico illecito di sostanze stupefacenti e psicotrope, approvata a Vienna il 19 dicembre 1988. Sebbene l'obiettivo di tale provvedimento sovranazionale fosse quello di individuare linee minimali per la lotta al traffico di stupefacenti, prevedeva l'impegno a stabilire sanzioni penali nei confronti di una serie di comportamenti particolarmente pericolosi per la comunità internazionale, tra cui, al par. 3 (1) (a), il riciclaggio. La definizione di riciclaggio ivi contenuta, sebbene indissolubilmente legata alla produzione, al traffico ed alla distribuzione di sostanze stupefacenti, nonché eccessivamente ampia[40], al punto da comprendere tra le condotte da criminalizzare anche il mero possesso di proventi illeciti, è diventata un punto di riferimento per gli Stati aderenti, nonché per gli strumenti internazionali successivamente adottati[41].

Altra importante iniziativa adottata in materia di lotta al riciclaggio sono le "Quaranta Raccomandazioni" adottate dal Gruppo d'Azione Finanziaria Internazionale (GAFI), costituito a Parigi nel luglio del 1989, che oggi costituisce il più autorevole organo internazionale per la formulazione di politiche antiriciclaggio e che ogni anno pubblica un rapporto sull'evoluzione della lotta al riciclaggio nel mondo[42]. Ai fini dell'applicazione delle Raccomandazioni viene indicata come descrizione tassativa del riciclaggio proprio quella contenuta nella menzionata Convenzione di Vienna del 1988. Le "Quaranta Raccomandazioni" nel corso degli anni sono state riviste diverse volte, al fine di adeguarle

[38] PING H., *New Trends in Money Laundering – From the Real Word to Cyberspace*, in *J. Money Laund. Control*., 2004, vol. 8, n. 1, p. 48 ss.
[39] DIBIAGIO T.M., *Money Laundering and Drug Trafficking: A Question of Understanding the Elements of the Crime and the Use of Circumstantial Evidence*, in *U. Rich. L. Rev.*, 1994, vol. 28, p. 255 ss., p. 256.
[40] DELL'OSSO A.M., *Riciclaggio Di Proventi Illeciti*, cit., p. 11, che evidenzia come la formula ivi proposta sovrappone condotte che costituiscono vero e proprio riciclaggio a fatti di favoreggiamento.
[41] POLIMENI G., *La concertazione internazionale*, in E. Palombi (a cura di), *Il riciclaggio dei proventi illeciti. Tra politica criminale e diritto vigente*, Napoli, 1996, p. 59 ss., p. 62.
[42] FAIELLA S., *Riciclaggio e crimine organizzato transnazionale*, Milano, 2009, p. 37. Per approfondire in merito alle iniziative del GAFI v. https://www.fatf-gafi.org/

alle nuove tecniche utilizzate per commettere il riciclaggio di denaro e anticipare le nuove possibili minacce. Inoltre, lo stesso GAFI prevede un meccanismo di implementazione ed applicazione delle Raccomandazioni che gli Stati aderenti al progetto devono seguire[43].

Altra importante misura sovranazionale è costituita dalla Convenzione sul riciclaggio, la ricerca, il sequestro e la confisca dei proventi di reato del Consiglio d'Europa, firmata a Strasburgo l'8 novembre 1990, che all'art. 6 fornisce una definizione di "reati di riciclaggio" non limitata al traffico di stupefacenti, bensì estesa ad un ampio catalogo di reati presupposto. Tale Convenzione prevede diverse disposizioni in ordine alla cooperazione internazionale, in particolare in merito all'assistenza alle indagini, all'adozione di misure provvisorie quali il congelamento ed il sequestro, nonché l'obbligo della confisca su richiesta. Essa, inoltre, ha introdotto l'obbligo di introdurre negli ordinamenti nazionali il reato di riciclaggio, richiamando anch'essa la nozione fornita dalla citata Convenzione di Vienna del 1988, ma riferita non più unicamente ai reati in materia di stupefacenti, bensì a tutti i reati o comunque ai reati più gravi[44]. Altra peculiarità del provvedimento in questione è che l'art. 6 specifica che non ha importanza che l'attività illecita cui i proventi sono oggetto di riciclaggio costituisca reato anche nello Stato in cui i proventi vengono riciclati. Inoltre, ha previsto la possibilità per i singoli Stati aderenti di punire il riciclaggio a titolo di colpa[45].

Tutti i documenti internazionali indicati si caratterizzano per il fatto che, nonostante la sua particolare ampiezza, la definizione normativa di riciclaggio è tutt'altro che precisa. Tale carenza di tassatività è almeno in parte funzionale alle esigenze di una comunità multistatale, che non ha una politica criminale organica ben definita[46]. Ciò, infatti, ha consentito a ciascuno Stato membro di costruire le proprie fattispecie incriminatrici in materia con estrema discrezionalità, agevolando l'adesione agli strumenti citati e l'incriminazione del fenomeno[47].

Anche il legislatore europeo si è mostrato sensibile in merito alla necessità di adottare iniziative congiunte tra i Paesi membri per la lotta al fenomeno del riciclaggio di denaro. Il primo provvedimento adottato è stata la direttiva del Consiglio del 10 giugno 1991, n. 91/308/CEE, che, anch'essa, prende spunto dalla citata Convenzione di Vienna e che all'art. 1 definisce le condotte di riciclaggio. Essa fu adottata allo scopo istituire misure di

[43] Sul punto v. DÍAZ-MAROTO Y VILLAREJO J., *Recepción de las propuestas del GAFI y de las directivas europeas sobre el blanqueo de capitales en el derecho español*, in M. Bajo Fernández, S. Bacigalupo Saggese (a cura di), *Política Criminal y blanqueo de capitales*, Madrid, 2009, p. 21 ss., p. 32 ss.
[44] AMATO G., *Il riciclaggio del denaro "sporco"*, cit., p. 120.
[45] NILSSON H.G., *The Council of Europe Laundering Convention*, cit., p. 431.
[46] ZANCHETTI M., *Il riciclaggio di denaro*, cit., p. 164.
[47] POLIMENI G., *La concertazione internazionale*, cit., p. 63.

coordinamento a livello comunitario per contrastare il fenomeno del riciclaggio di denaro, armonizzando la legislazione dei diversi Stati membri ed è la prima iniziativa sovranazionale riferita al riciclaggio di denaro che ha obbligato gli Stati membri ad adattare le loro legislazioni nazionali al diritto europeo entro un dato termine[48]. Tale prima direttiva ha carattere amministrativo, non penale, e ha introdotto diversi obblighi diretti agli Stati membri riferiti alla collaborazione e al controllo del sistema finanziario, prevedendo in particolare l'obbligo per enti finanziari e creditizi di identificare i loro clienti nelle determinate situazioni descritte nella direttiva[49]. Essa contiene poi all'art. 1 contiene una definizione dell'attività di riciclaggio, ossia la conversione o nel trasferimento di beni, effettuati essendo a conoscenza del fatto che essi provengono da un'attività criminosa o da una partecipazione a tale attività, allo scopo di occultare o dissimulare l'origine illecita dei beni medesimi o di aiutare chiunque sia coinvolto in tale attività a sottrarsi alle conseguenze giuridiche delle proprie azioni; nell'occultamento o nella dissimulazione della reale natura, provenienza, ubicazione, disposizione, movimento, proprietà dei beni o diritti sugli stessi; nell'acquisto, nella detenzione o nell'utilizzazione di beni nel concorso in uno degli atti di cui ai punti precedenti, nella partecipazione all'associazione per commettere tale atto, nel tentativo di perpetrarlo, nel fatto di aiutare, istigare o consigliare qualcuno a commetterlo o il fatto di agevolarne l'esecuzione. Come si esaminerà meglio nel capitolo successivo (v. cap. V, par. 8), tale definizione, praticamente identica a quella contenuta nella già esaminata Convenzione di Vienna del 1988, ha avuto notevole influenza nell'introduzione delle fattispecie di riciclaggio nei diversi ordinamenti europei, in particolare con riferimento alla scelta delle condotte da sanzionare.

Tale direttiva fu poi modificata dalla direttiva 2001/97/CE, con la quale fu ampliata la definizione di "enti finanziari", l'elenco dei soggetti obbligati ai sensi della normativa in esame nonché l'elenco dei reati presupposto per il riciclaggio. Con tale provvedimento, si è, dunque, preso atto che ad avere un ruolo di rilievo nel riciclaggio non sono unicamente le istituzioni bancarie, ma anche altre istituzioni non finanziarie operanti in altri settori ove si può mescolare il denaro sporco ai ricavi leciti, quali ad esempio i casinò[50].

Con la terza direttiva antiriciclaggio 2005/60/CE, relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di

[48] SEOANE PEDREIRA A., *El delito del blanqueo de dinero: Historia, práctica jurídica y técnicas de blanqueo*, Cizur Menor, 2017, p. 80.
[49] *Ibid*., p. 81.
[50] PING H., *New Trends in Money Laundering*, cit., p. 49; MANES V., *Il riciclaggio dei proventi illeciti*, cit., p. 39.

finanziamento del terrorismo, l'ambito applicativo della normativa antiriciclaggio fu poi ampliato anche alla prevenzione del finanziamento al terrorismo. Inoltre, è stato introdotto per la prima volta l'obbligo di adottare mezzi di verifica della clientela, a partire dalla loro identificazione. Tali mezzi di verifica sono diversi per ciascuna tipologia di cliente, dipendendo dall'operazione realizzata e dalla tipologia della transazione e ad ognuna delle tipologie si accompagnano tre diversi livelli di diligenza richiesta da parte dei soggetti obbligati: semplificati, ordinari o rafforzati.

La quarta direttiva antiriciclaggio, ovvero la direttiva 2015/849/UE, ha poi stabilito che anche i reati tributari rientrano tra i reati presupposto del riciclaggio, ha creato una "lista nera" comunitaria di Paesi terzi c.d. ad alto rischio al fine di proteggere il buon funzionamento del mercato interno, ha ridotto l'importo per cui è possibile pagare in contanti, ampliato il controllo sulle transazioni effettuate nel settore del gioco d'azzardo e, infine, ha esonerato determinati soggetti obbligati in virtù delle direttive precedenti dall'obbligo di verificare l'identità del cliente nell'ambito di determinate attività, quali la difesa nel procedimento giudiziale. Per adeguare la propria legislazione a tale direttiva, il nostro legislatore ha ampiamente modificato il d.lgs. 231/2007, prevedendo indicatori più precisi relativi alla presenza del rischio di riciclaggio, estendendo il novero delle c.d. "persone politicamente esposte" nonché il concetto di "importanti cariche pubbliche" ed ampliando il novero dei soggetti obbligati ai sensi della normativa antiriciclaggio. Tuttavia, il legislatore italiano non si è limitato unicamente alla modifica delle disposizioni amministrative, ma ha anche integralmente sostituito l'art. 55 del d.lgs.21 novembre n. 231/2007, il quale, come si esaminerà meglio nel prosieguo (v. *infra* par. 3.4), prevede diverse disposizioni sanzionatorie per il caso di inadempimento degli obblighi antiriciclaggio previsti dalle disposizioni in materia.

L'ultima direttiva adottata in tale ambito è la quinta direttiva 2018/843/UE. Con tale provvedimento il legislatore europeo ha preso atto della popolarità e diffusione tra il pubblico dei sistemi finanziari alternativi, non controllati né dallo Stato né dalle banche centrali. Pertanto, ha inserito tra i soggetti obbligati ai sensi della normativa antiriciclaggio anche i prestatori di servizi di cambio tra valute virtuali e valute legali (*exchange*), nonché i prestatori di servizi di portafoglio digitale[51]. Questi ultimi, ai sensi del nuovo numero 19) aggiunto all'art. 3 della direttiva 2015/849/UE dall'art. 1 della direttiva 2018/843/UE,

[51] FROMBERG M., HAFFKE L., ZIMMERMANN P., *Kryptowerte und Eine Analyse der 5. Geldwäscherichtlinie sowie des Gesetzesentwurfs der Bundesregierung*, in *BKR*, 2019, p. 377 ss., p. 377 ss.

vengono definiti come "un soggetto che fornisce servizi di salvaguardia di chiavi crittografiche private per conto dei propri clienti, al fine di detenere, memorizzare e trasferire valute virtuali". Infatti, come emerge dal *Considerando* n. 9 della direttiva, la maggior preoccupazione del legislatore europeo è dovuta all'anonimato delle valute virtuali, che consente agevolmente l'utilizzazione delle stesse per scopi criminali[52]. Lo stesso legislatore europeo riconosce che questa misura non può essere risolutiva, visto che le valute virtuali consentono agli utenti di effettuare operazioni anche senza l'aiuto di intermediari. Tuttavia, ha ritenuto di dover comunque cercare di contrastare i rischi legati all'anonimato.

A tal proposito, si deve sottolineare che il nostro legislatore, anticipando l'orientamento del legislatore comunitario, aveva già ampliato la platea dei soggetti obbligati, dato che il d.lgs. 25 maggio 2017, n. 90 aveva inserito tra i soggetti tenuti al rispetto della normativa antiriciclaggio anche "i prestatori di servizi relativi all'utilizzo di valuta virtuale, limitatamente allo svolgimento dell'attività di conversione di valute virtuali da ovvero in valute aventi corso forzoso".

La direttiva in esame fornisce poi la seguente definizione di valuta virtuale: «*una rappresentazione di valore digitale che non è emessa o garantita da una banca centrale o da un ente pubblico, non è necessariamente legata a una valuta legalmente istituita, non possiede lo status giuridico di valuta o moneta, ma è accettata da persone fisiche e giuridiche come mezzo di scambio e può essere trasferita, memorizzata e scambiata elettronicamente*». Tale definizione è stata poi integralmente ripresa dalla già esaminata direttiva 2019/713/UE relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti.

Il legislatore europeo ha poi voluto limitare la prassi di utilizzo delle carte prepagate anonime, che possono essere utilizzate per scopi criminali, riducendo ulteriormente i limiti e gli importi massimi al di sotto dei quali i soggetti obbligati sono autorizzati a non applicare determinate misure di adeguata verifica della clientela. Pertanto, ha previsto la facoltà per gli Stati membri di decidere di non accettare sul proprio territorio i pagamenti effettuati utilizzando carte prepagate anonime.

---

[52] «*L'anonimato delle valute virtuali ne consente il potenziale uso improprio per scopi criminali. L'inclusione dei prestatori di servizi la cui attività consiste nella fornitura di servizi di cambio tra valute virtuali e valute reali e dei prestatori di servizi di portafoglio digitale non risolve completamente il problema dell'anonimato delle operazioni in valuta virtuale: infatti, poiché gli utenti possono effettuare operazioni anche senza ricorrere a tali prestatori, gran parte dell'ambiente delle valute virtuali rimarrà caratterizzato dall'anonimato. Per contrastare i rischi legati all'anonimato, le unità nazionali di informazione finanziaria (FIU) dovrebbero poter ottenere informazioni che consentano loro di associare gli indirizzi della valuta virtuale all'identità del proprietario di tale valuta. Occorre inoltre esaminare ulteriormente la possibilità di consentire agli utenti di presentare, su base volontaria, un'autodichiarazione alle autorità designate*».

Tale ultima direttiva è stata recepita nel nostro ordinamento dal d.lgs. 4 ottobre 2019, n. 125, con il quale è stata ulteriormente ampliata la platea dei destinatari della normativa antiriciclaggio, inserendovi, oltre ai già presenti prestatori di servizi relativi all'utilizzo di valuta virtuale, anche i prestatori di servizi di portafoglio digitale. Inoltre, all'art. 3 è stato aggiunto il divieto di emissione e utilizzo di prodotti di moneta elettronica anonimi, non espressamente previsto dalla direttiva antiriciclaggio[53]. Infine, come già evidenziato (v. *supra*, cap. I par. 3), nel recepire la direttiva il nostro legislatore ha inserito all'art. 1 lett. qq) del d.lgs. 21 novembre 2007, n. 231 la nuova definizione di valuta virtuale, la quale, però, si differenzia rispetto a quella fornita dal legislatore comunitario, perché aggiunge espressamente anche la finalità di investimento, discrasia che non è certo di aiuto per l'identificazione della natura giuridica di tali strumenti.

A partire dalla prima direttiva fino all'ultima del 2018, dunque, il legislatore europeo ha progressivamente costruito e in seguito affinato un reticolo di obblighi posti a carico di enti finanziari e creditizi, nonché di ulteriori soggetti privati ritenuti in una conveniente situazione di prossimità rispetto al riciclaggio. Non solo, ma nel corso dei vari provvedimenti ha costantemente ampliato la lista dei reati presupposto necessari a commettere riciclaggio di denaro, fino ad arrivare ad accogliere il c.d. paradigma *all-crime*[54].

Si evidenzia poi che il riciclaggio è espressamente menzionato tra le "sfere di criminalità particolarmente grave che presentano una dimensione transnazionale" di cui all'art. 83 co. 1 TFUE, che legittimano l'adozione di direttive in materia penale per stabilire norme minime relative alla definizione dei reati e delle sanzioni. Il legislatore europeo ha fatto uso di questa competenza con la direttiva 2018/1673/UE. Tale direttiva ha sostituito alcune delle disposizioni della decisione quadro 2001/500/GAI, concernente il riciclaggio di denaro, l'individuazione, il rintracciamento, il congelamento o sequestro e la confisca degli strumenti e dei proventi di reato, provvedimento che era stato adottato allo scopo di rafforzare la cooperazione degli Stati membri in merito all'identificazione, al tracciamento ed alla confisca dei proventi di reato[55]. La direttiva 2018/1673/UE all'art. 3, intitolato "riciclaggio" prevede una serie di condotte che gli Stati membri devono obbligatoriamente sanzionare penalmente. In particolare, si menzionano alla lett. a) del par. 1 la conversione o

[53] Per una disamina complete delle modifiche apportate al d.lgs. 21 novembre 2007, n. 231 dal d.lgs. 4 ottobre 2019, n. 125 v. VADALÁ R.M., *Criptovalute e cyberlaundering: novità antiriciclaggio nell'attesa del recepimento della Direttiva (UE) 2018/1673 sulla lotta al riciclaggio mediante il diritto penale*, in *Sist. pen*, 6 maggio 2020.
[54] MITSILEGAS V., VAVOULA N., *The evolving EU anti-money laundering regime: challenges for fundamental rights and the rule of law*, in *Maastricht J. Eur. & Comp. L.*, 2016, vol. 23, n. 2, p. 261 ss., p. 269.
[55] STESSENS G., *Money laundering*, in *Rev. Int. de Droit Penal*, 2006, vol. 77, p. 201 ss., p. 207.

il trasferimento di beni, effettuati essendo nella consapevolezza che i beni provengono da un'attività criminosa, allo scopo di occultare o dissimulare l'origine illecita dei beni medesimi o di aiutare chiunque sia coinvolto in tale attività a sottrarsi alle conseguenze giuridiche della propria condotta. Alla lett. b), invece, si fa riferimento all'occultamento o alla dissimulazione della reale natura, della provenienza, dell'ubicazione, della disposizione, del movimento, della proprietà dei beni o dei diritti sugli stessi nella consapevolezza che i beni provengono da un'attività criminosa.

Oltre a tali condotte, che si caratterizzano per essere idonee ad ostacolare l'identificazione della provenienza delittuosa del bene, la norma in questione impone anche la punizione di condotte c.d. neutre, quali «*l'acquisto, la detenzione o l'utilizzazione di beni nella consapevolezza, al momento della loro ricezione, che i beni provengono da un'attività criminosa*». Questo perché la definizione europea di riciclaggio, essendo mutuata da quella molto ampia prevista dalla Convenzione di Vienna, è sempre stata molto vasta e comprensiva di tutte le varie condotte di *placement*, *layering* ed *integration*, comprese quelle sopra descritte[56]. Questa eccessiva ampiezza, però comporta una significativa estensione dell'ambito applicativo della fattispecie di riciclaggio, perché, a differenza di quanto previsto dalla Convenzione di Vienna, non è lasciata alcuna discrezionalità in capo agli Stati membri, che sono obbligati a conformarsi a tale disposizione e a sanzionare penalmente le condotte ivi descritte. Tale previsione, come si esaminerà meglio nel prosieguo, è foriera di problemi e difficoltà, trattandosi di condotte difficilmente assimilabili al riciclaggio.

L'art. 3 par. 5 ha poi per la prima volta espressamente imposto l'obbligo di punire come reato anche le condotte commesse dall'autore del reato presupposto, purché non siano limitate alla mera detenzione o utilizzazione dei beni. La direttiva, inoltre, si occupa anche della questione della giurisdizione, prevedendo all'art. 10 par. 1 lett. b) anche l'obbligo per gli Stati membri di stabilire la propria giurisdizione nazionale nel caso in cui l'autore dei reati di cui agli artt. 3 e 4 della direttiva sia un proprio cittadino.

A seguito di questa breve analisi è già possibile effettuare un primo bilancio. Sul piano della tecnica legislativa in materia di riciclaggio, si può notare che i provvedimenti internazionali, legislativi o meno, aspirano tutti ad essere capillari, tendenti alla "completezza" e alla flessibilità per tenere il passo con la costante evoluzione delle operazioni di riciclaggio. Questa tecnica presenta un notevole inconveniente, perché la

[56] MORABITO M.A., *Lo schema di decreto legislativo per l'attuazione della direttiva UE 2018/1673 sulla lotta al riciclaggio mediante il diritto penale: analisi e considerazioni*, in *Giur. pen. web.*, 2021, n. 9, p. 1 ss., p. 5.

flessibilità, capillarità e rapida evoluzione del sistema normativo presuppongono che sia la giurisprudenza a trovare il giusto equilibrio tra l'efficace applicazione della normativa antiriciclaggio ed il rispetto dei principi dello Stato di diritto[57]. Ciò è dovuto al fatto che, come sopra evidenziato, gli strumenti internazionali cui la normativa antiriciclaggio dei Paesi europei si è ispirata o adeguata sono stati notevolmente influenzati dall'esempio nordamericano. Dunque, le fattispecie penali di riciclaggio presenti in molti ordinamenti europei sono formulate secondo una tecnica legislativa tipicamente nordamericana, che, ad esempio, in maniera contraria alla tradizione giuridica europea, equipara tra loro gli atti preparatori, il tentativo e la consumazione[58]. Ma, come si esaminerà meglio nel prosieguo, la nostra legislazione in materia costituisce un'eccezione. Infatti, nonostante l'elevato numero di fattispecie, le condotte sanzionate restano limitate rispetto a quelle punite da altri legislatori europei quali quello tedesco e spagnolo e, soprattutto, riferite a comportamenti idonei a mascherare l'origine illegale dei proventi.

3. Le fattispecie in materia di riciclaggio presenti nel codice penale

La prima norma antiriciclaggio introdotta nel codice penale italiano risale al 1978. Con il d.l. 21 marzo 1978, n. 59, convertito con modificazioni nella l. 18 maggio 1978, n. 191, fu, infatti, introdotto l'art. 648-*bis* c.p., ovvero la prima fattispecie diretta specificamente a reprimere l'attività di riconversione dei beni di provenienza illecita, per impedire che questi fossero reimmessi sul mercato[59]. Fu collocata nel codice immediatamente dopo il delitto di ricettazione, dunque tra i reati contro il patrimonio, per cui secondo l'originaria impostazione essa era inquadrabile nell'ambito della sua tutela[60]. Inizialmente tale fattispecie aveva quale rubrica "sostituzione di denaro o valori provenienti da rapina aggravata, estorsione aggravata o sequestro di persona a scopo di estorsione" ed era pensata come norma volta a contrastare il fenomeno dei sequestri di persona. Non era qualificato come fenomeno criminoso autonomo, tant'è che i reati presupposto erano limitati alla rapina aggravata, all'estorsione aggravata ed al sequestro di persona a scopo di estorsione[61]. Non solo, ma nella prima formulazione della norma non era presente nessun riferimento all'ostacolo all'identificazione della provenienza del bene[62]. In ogni caso,

[57] ZANCHETTI M., *Il riciclaggio di denaro*, cit., p. 326 s.
[58] NIETO MARTÍN A., *¿Americanización o europeización del derecho penal económico?*, in *Rev. pen.*, 2007, n. 19, p. 120 ss., p. 130.
[59] AMATO G., *Il riciclaggio del denaro "sporco"*, cit., p. 117.
[60] FAIELLA S., *Riciclaggio e crimine organizzato transnazionale*, cit., p. 36.
[61] DELL'OSSO A.M., *Riciclaggio Di Proventi Illeciti*, cit., p. 6.
[62] FAIELLA S., *Riciclaggio e crimine organizzato transnazionale*, cit., p. 19.

nonostante la stringente limitazione ad un piccolo numero di reati presupposto, essa si caratterizzava per l'anticipazione della tutela penale, dato che sanzionava anche i semplici atti o fatti diretti alla sostituzione, senza che fosse necessaria l'effettiva sostituzione del denaro o dei valori[63].

Nel tempo vi sono state numerose novelle legislative, che hanno profondamente mutato la struttura della normativa penale antiriciclaggio. Oggi le fattispecie che puniscono il riciclaggio in senso lato sono due. Il nostro legislatore, infatti, a differenza di quasi tutti gli altri legislatori nazionali, ha preferito "scomporre" il fenomeno in modo da distinguere le fasi di collocamento e ripulitura da quelle di riutilizzo nel sistema economico[64]. Questo perché ha seguito in modo rigoroso il modello adottato dalla Convenzione ONU di Vienna e gli atti internazionali successivi che da essa hanno preso le mosse, che distinguono con chiarezza tra penalizzazione dei reati base, riciclaggio e reimpiego. Le condotte relative al riciclaggio, infatti, nella formulazione delle organizzazioni internazionali sono ripartite in due categorie: da un lato la "sostituzione" o il "trasferimento" dei beni provenienti da reato", dall'altro "l'occultamento" o la "dissimulazione" dell'origine criminosa dei beni. Questi comportamenti a loro volta vengono tenuti distinti dall'"impiego" di beni di provenienza delittuosa, cui viene equiparato "l'acquisto" di tali beni[65].

Le fattispecie italiane di "riciclaggio" di cui all'art. 648-*bis* c.p. e impiego ex art. 648-*ter* c.p. così come riformulate dalla l. 8 marzo 1990, n. 55 e dalla l. 9 agosto 1993, n. 328 rispecchiano in modo fedele la ripartizione delle condotte proposta negli atti sovranazionali[66]. Vi è chi ha criticato la partizione dell'attività criminosa in due fasi distinte, evidenziando che la stessa non risponde alla fenomenologia del riciclaggio, che è fenomeno unitario e multifasico, per cui spesso è impossibile distinguere tra ipotesi di "solo" lavaggio e ipotesi di "solo" impiego. Ciò rende improduttiva la ripartizione del riciclaggio in due norme che mirano a punire comportamenti intesi come temporalmente sfasati[67].

Nonostante l'omologazione, a seguito della novella di cui alla l. 328/1993, di molti degli elementi previsti dai delitti di ricettazione, riciclaggio ed impiego, il rapporto di specialità tra le tre fattispecie non è affatto venuto meno, cosa che, invece, come si esaminerà meglio nel prosieguo, non può affatto ritenersi per altri ordinamenti europei. La condotta della ricettazione di cui all'art. 648 c.p., infatti, consiste genericamente nell'acquistare,

[63] AMATO G., *Il riciclaggio del denaro "sporco"*, cit., p. 122.
[64] SCAPELLATO F., *Il fenomeno del riciclaggio e la normativa di contrasto*, Torino, 2013, p. 33.
[65] ZANCHETTI M., *Il riciclaggio di denaro*, cit., p. 165.
[66] *Ibid*., p. 166.
[67] *Ibid*., p. 168 s.

ricevere od occultare la cosa, lasciandone inalterata la sua identità fisica. Viceversa, nel riciclaggio la condotta sanzionata è diretta proprio ad alterare tale identità mediante operazioni dirette ad ostacolarne l'identificazione. Ancora, la norma di cui all'art. 648-*ter* c.p. interviene a sanzionare l'impiego in attività economiche o finanziarie delle cose provenienti dai delitti presupposti[68].

A queste due fattispecie penali è stata aggiunta la fattispecie di autoriciclaggio, inserita quale art. 648-*ter*.1 c.p. dalla l. 15 dicembre 2014, n. 186. Infatti, le fattispecie di riciclaggio ed impiego di denaro, beni o utilità di provenienza illecita di cui agli artt. 648-*bis* c.p. e 648-*ter* c.p., in modo analogo alla ricettazione, si applicano entrambi «*fuori dei casi di concorso nel reato*». Tale clausola di riserva impone che il riciclatore non abbia concorso alla realizzazione del reato presupposto. Prima dell'introduzione della norma in questione, dunque, vi era il c.d. privilegio di autoriciclaggio, frutto dell'equiparazione della fattispecie di riciclaggio a quella di ricettazione, per cui si riteneva che la condotta volta a nascondere l'origine illegale dei beni commessa dall'autore del reato presupposto fosse un post *factum* non punibile[69]. La criminalizzazione dell'autoriciclaggio, infatti, comporta il rischio di conflitto coi principi del *ne bis in idem* e del *nemo tenetur se detegere*, perché si rischia di sanzionare fatti che rappresentano la necessaria evoluzione del reato presupposto o che rientrano in una strategia difensiva, volta ad evitare che si venga a conoscenza dell'illecita provenienza del bene[70]. Nonostante ciò, plurime sollecitazioni, provenienti anche dall'OCSE e dal Fondo Monetario Internazionale[71], indussero il legislatore a superare il c.d. privilegio di autoriciclaggio ed introdurre una fattispecie *ad hoc* volta a reprimere anche questa manifestazione criminosa.

A completare il quadro normativo delle disposizioni penali in materia di antiriciclaggio vi sono poi le fattispecie relative all'ostacolo e prevenzione dei fenomeni del riciclaggio e di reimpiego dei capitali illeciti. Introdotte dal d.l. 3 maggio 1991, n. 143, convertito dalla l. 5 luglio 1991, n. 197, sono oggi previste dall'art. 55 del d.lgs. 21 novembre 2007, n. 231 e sanzionano il mancato rispetto di obblighi di segnalazione e di identificazione della clientela.

---

[68] PATALANO V., *Profili della repressione penale del riciclaggio*, in E. Palombi (a cura di), *Il riciclaggio dei proventi illeciti. Tra politica criminale e diritto vigente*, Napoli, 1996, p. 313 ss., p. 321.
[69] SEMINARA S., *I soggetti attivi del reato di riciclaggio tra diritto vigente e proposte di riforma*, in *Dir. pen. proc.*, 2005, n. 2, p. 233 ss., p.
[70] DELL'OSSO A.M., *Riciclaggio Di Proventi Illeciti*, cit., p. 173.
[71] BRICCHETTI R., *Riciclaggio e auto-riciclaggio*, in *Riv. it. dir. proc. pen.*, 2014, n. 2, p. 684 ss., p. 693.

Dunque, il quadro normativo antiriciclaggio nel nostro ordinamento si articola su tre direttive. La prima è di tipo preventivo, contenuta nella legislazione complementare che, come appena visto, prevede la presenza di un complesso sistema di controlli sulla circolazione del denaro e sull'attività d'intermediazione finanziaria. La seconda, invece, è di tipo repressivo tradizionale, affidata a fattispecie incriminatrici contenute nel codice penale. La terza, infine, attiene alla sfera successiva al delitto e si esprime nella previsione di una serie di misure di sequestro e confisca dei proventi illeciti, che costituiscono il capitale d'impiego dell'impresa criminale[72].

Le disposizioni sopra elencate, dunque, vanno ora esaminate nel dettaglio.

3.1. Il riciclaggio ex art. 648-*bis* c.p.

L'art. 648-*bis* c.p. fu introdotto nel codice penale dal d.l. 21 marzo 1978 n. 59, convertito dalla l. 18 maggio 1978. La norma fu poi sostanzialmente modificata sia dalla l. 19 marzo 1990, n. 55 che dalla l. 9 agosto 1993, n. 328. Ulteriori modifiche sono state infine apportate dal d.lgs. 8 novembre 2021, n. 195, di recepimento della direttiva 2018/1673/UE sulla lotta al riciclaggio mediante il diritto penale.

L'individuazione del bene giuridico tutelato dalla norma in questione è stata oggetto di ampia discussione in dottrina. Inizialmente, data la collocazione della norma, un settore della dottrina riteneva che essa integrasse un reato contro il patrimonio[73]. Per altri autori si tratterebbe di un reato a tutela dell'ordine economico[74], mentre per altri ancora il principale oggetto di tutela andrebbe individuato nell'amministrazione della giustizia[75]. Oggi, però, per l'opinione largamente maggioritaria si tratta di fattispecie plurioffensiva, che lede l'economia, l'ordine pubblico, l'amministrazione della giustizia, oltre che il patrimonio[76]. La plurioffensività rende il delitto più grave rispetto alla ricettazione e giustifica il fatto che le pene previste siano più elevate[77].

A seguito della riforma del 1990 l'oggetto materiale del riciclaggio è costituito da "denaro, beni o altre utilità". L'allargamento del raggio di azione della norma è stato voluto

---

[72] MOCCIA S., *Impiego di capitali illeciti e riciclaggio: la risposta del sistema penale italiano,* in *Riv. it. dir. proc. pen*., 1995, n. 3, p. 728 ss., p. 729.
[73] MOCCIA S., *Tutela penale del patrimonio e principi costituzionali*, cit., p. 62.
[74] FLICK G.M., *La repressione del riciclaggio ed il controllo dell'intermediazione finanziaria. Problemi attuali e prospettive,* in *Riv. it. dir. proc. pen*., 1990, n. 4, p. 1255 ss., p. 1262.
[75] MANES V., *Il riciclaggio dei proventi illeciti*, cit., p. 59; ZANCHETTI M., *Il riciclaggio di denaro,* cit., p. 387 ss.; FAIELLA S., *Riciclaggio e crimine organizzato transnazionale*, cit., p. 233.
[76] ANTOLISEI F., *Manuale di diritto penale. PS*, cit., p. 463; FIANDACA G., MUSCO E., *Diritto penale. PS*., vol. III, cit., p. 247.
[77] SCAPELLATO F., *Il fenomeno del riciclaggio*, cit., p. 36.

per fugare ogni dubbio sull'inclusione nell'oggetto del riciclaggio di beni immobili, crediti, beni immateriali e di ogni altra utilità che possa provenire da reato ed essere riciclata nel mercato lecito[78]. A tal proposito, va sottolineato che l'art. 1 della prima direttiva antiriciclaggio forniva una definizione di beni oggetto di riciclaggio comprensiva di «*beni di qualsiasi tipo, materiali o immateriali, mobili o immobili, tangibili o intangibili e i documenti o gli strumenti legali che attestano il diritto di proprietà o diritti sui beni medesimi*», definizione che oggi è stata ripresa dall'art. 2 n. 2) della direttiva 2018/1673/UE sulla lotta al riciclaggio mediante il diritto penale, la quale specifica che ai fini della propria attuazione devono considerarsi rilevanti proprio i beni ivi indicati. La formulazione della norma, dunque, è certamente coerente con gli obiettivi perseguiti dal legislatore europeo. Per quanto riguarda specificamente le criptovalute, va evidenziato che l'art 2 n. 2) della direttiva 2018/1673/UE alla nozione di beni oggetto di riciclaggio già contenuta nell'art. 1 della prima direttiva antiriciclaggio ha espressamente aggiunto che i beni possono essere «*in qualsiasi forma, compresa quella elettronica o digitale*». Alcuni autori, dunque, hanno criticato la scelta del nostro legislatore, in sede di attuazione della direttiva, di non ricomprendere espressamente nell'oggetto dei reati in esame anche le valute virtuali[79]. Si è, infatti, evidenziato che il tradizionale orientamento in materia di ricettazione ritiene pacificamente che i beni immateriali possano essere oggetto di tutela ai sensi dell'art. 648 c.p. solo qualora siano trasfusi in un documento o in una scrittura, rappresentativi o dimostrativi del diritto, con il rischio che le criptovalute, che altro non sono che un insieme di dati informatici, restino al di fuori dell'ambito applicativo della fattispecie[80]. Va però evidenziato che, a differenza del riciclaggio, oggetto della ricettazione sono le "cose", concetto diverso e non assimilabile ai "beni" e alle "altre utilità" di cui alla fattispecie di riciclaggio. In quest'ultimo caso il rischio paventato non sussiste. La definizione dell'oggetto del reato in questione, infatti, ha caratteristiche di onnicomprensività, tali da ricomprendere qualsiasi ipotizzabile provento di reato[81]. Peraltro, si è già evidenziato che le criptovalute, seppure non assimilabili alla moneta elettronica e che quindi non possono essere classificate come denaro o beni[82], hanno sicuro valore economico, potendo essere

[78] ZANCHETTI M., *Il riciclaggio di denaro*, cit., p. 396.
[79] PESTELLI G., *Riflessioni critiche sulla riforma dei reati di ricettazione, riciclaggio, reimpiego e autoriciclaggio di cui al d.lgs. 8 novembre 2021, n. 195*, in *Sist. Pen.*, 2021, n. 12, p. 49 ss., p. 61.
[80] *Ibid*.
[81] INSOLERA G., *Diritto penale e criminalità organizzata*, Bologna, 1996, p. 147; PECORELLA G., *Circolazione del denaro e riciclaggio*, in *Riv. it. dir. proc. pen*., 1991, n. 4, p. 1221 ss., p. 1227.
[82] Sul punto v. Corte di giustizia UE, V sez., sentenza 22 ottobre 2015, causa C-264/14: «*la valuta virtuale a flusso bidirezionale «bitcoin», che sarà cambiata contro valute tradizionali nel contesto di operazioni di cambio, non può essere qualificata come «bene materiale» ai sensi dell'articolo 14 della direttiva IVA, dato*

scambiate e/o acquistate in cambio di un corrispettivo in denaro. Pertanto, possono essere ricomprese tra le "altre utilità" di cui all'art. 648-*bis* c.p., poiché questa definizione comprende qualsiasi entità di valore economico[83].

I beni, il denaro o le altre utilità in questione debbono essere "provento" di reato. Il riciclaggio, dunque, è riconducibile alla categoria dei c.d. reati accessori, perché presuppone la previa realizzazione di un altro reato, al quale accede[84]. Il nostro legislatore ha eliminato l'elenco dei reati presupposto del riciclaggio sin dalla riforma del 1993, aderendo così al c.d. paradigma *all-crimes*. Attraverso tale modifica, in luogo del catalogo fu inserita la formula "qualsiasi delitto non colposo". Ciò ha comportato una notevole semplificazione probatoria, perché la presenza di un elenco di delitti presupposto specifici creava un notevole *impasse* applicativo, dato che era necessario provare che il riciclatore fosse a conoscenza della provenienza del denaro riciclato da uno degli specifici reati previsti[85]. Oggi, pertanto, ai fini della configurabilità del riciclaggio non è richiesta l'individuazione esatta del titolo di reato presupposto, anche se la giurisprudenza richiede che quest'ultimo debba essere individuato quantomeno nella sua tipologia[86]. Tuttavia, allo scopo di mitigare il trattamento sanzionatorio, è stata inserita anche una circostanza attenuante ad effetto speciale per i casi di riciclaggio di beni e denaro provenienti da delitti puniti con la reclusione inferiore nel massimo a cinque anni.

A seguito della riforma di cui al d.lgs. n. 195 del 2021, è stato eliminato l'inciso "non colposo" accanto alla parola "delitti". Pertanto, reato presupposto del riciclaggio può oggi essere qualsiasi reato, anche colposo. Inoltre, è stato aggiunto un nuovo co. 2, che prevede una pena diversa «*quando il fatto riguarda denaro o cose provenienti da contravvenzione punita con l'arresto superiore nel massimo a un anno o nel minimo a sei mesi*». Dunque, oggi non è più necessario che i reati presupposto siano necessariamente delitti.

L'ultimo co. dell'art. 648-*bis* c.p. specifica che la fattispecie di riciclaggio trova applicazione anche quando l'autore del riciclaggio non è imputabile o non è punibile, nonché quando manchi una condizione di procedibilità riferita a tale delitto. Il reato presupposto,

---

che, come rilevato dall'avvocato generale al paragrafo 17 delle sue conclusioni, questa valuta virtuale non ha altre finalità oltre a quella di un mezzo di pagamento».

[83] CROCE M., *Cyberlaundering e valute virtuali*, cit., p. 138; CAPACCIOLI S., *Criptovalute e bitcoin: un'analisi giuridica*, Milano, 2015, p. 252; STURZO L., *Bitcoin e riciclaggio 2.0*, cit., p. 24.

[84] Sui reati accessori v. DELOGU T., *Contributo alla teoria dei reati accessori*, in *Giust. pen.*, 1947, II, p. 321 ss. e MORGANTE G., *Il reato come elemento del reato. Analisi e classificazione del concetto di reato richiamato dalla fattispecie penale*, Torino, 2013, p. 65 ss.

[85] ZANCHETTI M., *Il riciclaggio di denaro*, cit., p. 418 s.

[86] Cass. pen., sez. II, sentenza 23 febbraio 2022, n. 6584; Cass. pen., sez. II, sentenza 23 novembre 2021, n. 46773; Cass. pen., sez. II, sentenza 28 maggio 2019, n. 29689.

inoltre, non dev'essere necessariamente accertato con sentenza irrevocabile, né è richiesto che i suoi autori siano stati individuati[87]. È però necessario che il reato presupposto sia già stato consumato al momento della condotta di riciclaggio[88]. Nulla si prevede, invece, per l'ipotesi in cui il reato presupposto sia stato commesso all'estero. Nonostante ciò, in assenza di indicazione contraria, la giurisprudenza della suprema Corte pacificamente ritiene che il riciclaggio sia punibile anche in quest'ultimo caso[89].

L'art. 648-*bis* c.p. sanziona tre distinte condotte: la sostituzione di denaro, beni o altre utilità, il trasferimento degli stessi nonché il compimento di altre operazioni idonee ad ostacolare l'identificazione dell'origine illecita dei proventi. Si tratta di norma a più fattispecie, per cui anche in caso di commissione di più condotte diverse tra quelle descritte si configurerà unicamente un reato[90].

La condotta di sostituzione è presente sin dall'originaria formulazione del 1978. Con essa si intendono tutte quelle attività volte a mettere danaro o altri beni "puliti" al posto di quelli provenienti da reato[91]. Pertanto, comprende tutte le misure volte a sostituire i beni illecitamente ottenuti con altri beni di origine lecita, rendendo così più difficile risalire al crimine e all'autore. La sostituzione si compone di due fasi, la prima delle quali è la ricezione. Quest'ultima, però, integra il reato di ricettazione, per cui per aversi sostituzione occorre una condotta ulteriore, che può connotarsi nei termini più vari[92]. Il termine "sostituire" viene da sempre interpretato in modo da comprendere anche il deposito bancario, in quanto, essendo il denaro un bene fungibile, una volta depositata la somma la banca si impegna a restituire l'equivalente[93].

Il trasferimento, invece, è modalità attuativa del riciclaggio introdotta con la riforma del 1993 per far fronte all'esigenza di punire i trasferimenti che non implicano sostituzione, bensì atti a "confondere le acque"[94]. Tale condotta non è altro che una *species* della

[87] ACQUAROLI R., *Il riciclaggio*, in C. Piergallini, F. Viganò, M. Vizzardi, A. Verri (a cura di), *I delitti contro la persona. Libertà personale, sessuale e morale, domicilio e segreti*, in *Trattato di diritto penale. Parte speciale*, diretto da G. Marinucci ed E. Dolcini, Padova, 2015, Vol. X, p. 903 ss., p. 920.
[88] DELL'OSSO A.M., *Sub Art. 648-bis c.p.*, in G. Forti, S. Seminara, G. Zuccalà (a cura di), *Commentario breve al codice penale*, 2016, Padova, p. 2318 ss., p. 2321.
[89] Così *ex multis* Cass. pen., sez. II, sentenza 14 luglio 2020, n. 23679; Cass. pen., sez. II, sentenza 29 ottobre 2012, n. 4212.
[90] INSOLERA G., *Diritto penale e criminalità organizzata*, cit., p. 149.
[91] PECORELLA G., *Circolazione del denaro e riciclaggio*, cit., p. 1231.
[92] INSOLERA G., *Diritto penale e criminalità organizzata*, cit., p. 149.
[93] ZANCHETTI M., *Il riciclaggio di denaro*, cit., p. 360.
[94] ZANCHETTI M., *Il riciclaggio di denaro*, cit., p. 362 evidenzia che comportamenti di questo tipo erano già puniti prima della riforma in questione, in quanto costituivano "ostacolo all'identificazione" della provenienza delittuosa del bene, per cui ritiene che la precisazione della punibilità dei trasferimenti sia più una questione di chiarezza che di sostanza.

sostituzione, dalla quale si distingue per il fatto che i valori di provenienza illecita non vengono sostituiti o scambiati, ma semplicemente spostati da un soggetto ad un altro, in modo da far perdere le tracce della loro provenienza e della loro destinazione[95]. Si evidenzia che al termine trasferimento dev'essere dato un significato differente rispetto all'acquisto, perché l'acquisto implica un trasferimento a sé, mentre il trasferimento consiste in uno spostamento del bene nel patrimonio altrui[96]. Inoltre, esso va interpretato come necessario passaggio interpersonale, non come semplice traslazione spaziale[97]. A tale tesi si può obiettare che anche lo spostamento fisico del bene può risolversi in un ostacolo alla sua tracciabilità. In realtà la questione è priva di rilevanza pratica, dato che lo spostamento materiale di un bene può comunque rientrare nell'alveo della fattispecie in esame[98].

L'ultima modalità della condotta, infatti, consiste nel "compimento di altre operazioni", ipotesi residuale che prevede l'occultamento dell'origine dei beni[99]. Pertanto, la norma ha un campo di applicazione molto ampio e qualsiasi azione che serva a nascondere l'origine criminale dei beni è sufficiente ad integrare il reato in esame. Trattasi, dunque, di reato a forma libera[100]. L'amplissima formulazione dell'art. 648-*bis* c.p., dunque, comprende anche condotte prive di rilevanza economico-imprenditoriale, in quanto esse sono limitate ad ostacolare l'identificazione del bene proveniente dal delitto presupposto[101]. Per questo motivo, dato che la clausola di chiusura è estremamente elastica e non richiede il compimento di nessuna specifica modalità tecnica, si può affermare che il reato in questione può sanzionare anche le condotte di *laundering* commesse *online*[102]. Dunque, anche se l'utilizzo del *web* per commettere riciclaggio è una modalità che risulta priva di considerazione normativa espressa, non vi è la necessità di introdurre nessuna nuova fattispecie *ad hoc*, trattandosi di condotta già sanzionata dalla norma[103].

A seguito della riforma del 1993, alla fine dell'elenco delle condotte sanzionate è stato aggiunto anche l'inciso "in modo da ostacolare l'identificazione della provenienza delittuosa", per evitare un'eccessiva dilatazione della fattispecie criminosa e distinguerla dal favoreggiamento reale di cui all'art. 379 c.p.[104]. Secondo l'opinione assolutamente

[95] AMATO G., *Il riciclaggio del denaro "sporco"*, cit., p. 130.
[96] ZANCHETTI M., *Il riciclaggio di denaro*, cit., p. 362
[97] INSOLERA G., *Diritto penale e criminalità organizzata*, cit., p. 149.
[98] DELL'OSSO A.M., *Riciclaggio Di Proventi Illeciti*, cit., p. 106.
[99] DELL'OSSO A.M., *Sub Art. 648-bis c.p.*, cit., p. 2322.
[100] Cass. pen., sez. II, sentenza 11 febbraio 2022, n. 9533.
[101] SEMINARA S., *I soggetti attivi del reato di riciclaggio*, cit., p. 241.
[102] PICOTTI L., *Profili penali del cyberlaundering*, cit., p. 608.
[103] PLANTAMURA V., *Il cybericiclaggio*, cit., p. 861.
[104] AMATO G., *Il riciclaggio del denaro "sporco"*, cit., p. 131.

maggioritaria l'inciso in questione qualifica tutte le condotte descritte dalla norma, non solo il compimento di altre operazioni[105]. Pertanto, anche la sostituzione e il trasferimento possono essere considerati punibili solo se svolti con la richiesta modalità[106]. Si evidenzia, infatti, che né la sostituzione, né il trasferimento sono condotte che si connotano in sé per una particolare carica lesiva, per cui l'individuazione del contenuto di lesività del riciclaggio viene rimandata proprio al successivo inciso in esame. In questo modo, la locuzione viene ad identificare il contenuto di offensività del reato: costituisce riciclaggio qualsiasi operazione compiuta in modo da ostacolare l'identificazione della provenienza delittuosa dei beni per cui, viceversa, l'azione non è punibile se non ostacola la ricostruzione del c.d. *paper trial*[107]. Tale tesi viene accolta anche in giurisprudenza, che ribadisce che altrimenti il fatto non può ricadere nell'ambito applicativo della norma in questione[108]. Dunque, l'idoneità lesiva del comportamento punito è richiesta dal legislatore per la punibilità e contribuisce a definire la condotta tipica[109]. In questo modo, la fattispecie si caratterizza per la struttura "a condotta pregnante", contrapposta a quella "a condotta neutra" adottata in altri ordinamenti europei[110]. Non manca, però, chi evidenzia come anche quest'ultimo inciso sia in realtà eccessivamente generico per fungere da criterio realmente selettivo[111].

Le condotte di riciclaggio sono rimaste immutate anche a seguito del d.lgs. 8 novembre 2021, n. 195, di recepimento della direttiva 2018/1673/UE. Infatti le condotte di cui alle lett. a) e b) della menzionata direttiva, ovvero la conversione o il trasferimento di beni, nonché l'occultamento o la dissimulazione della loro reale natura, origine, ecc. sono già ricomprese tra quelle sanzionate dalla norma. Va evidenziato, però, che, come in precedenza sottolineato, tra le condotte da incriminare la direttiva prevede anche l'acquisto, la detenzione o l'utilizzazione di beni nella consapevolezza, al momento della loro ricezione, che i beni provengono da un'attività criminosa. Tali condotte, tuttavia, non rientrano nell'ambito applicativo del reato di riciclaggio, bensì della diversa fattispecie di ricettazione ex art. 648 c.p. Questo reato, infatti, sanziona colui che acquista, riceve od occulta denaro o cose provenienti da un qualsiasi delitto, o, a seguito della riforma di cui al d.lgs. 8 novembre

[105] DELL'OSSO A.M., *Riciclaggio Di Proventi Illeciti*, cit., p. 109; ZANCHETTI M., *Il riciclaggio di denaro*, cit., p. 208; ACQUAROLI R., *Il riciclaggio*, cit., p. 912; AMATO G., *Il riciclaggio del denaro "sporco"*, cit., p. 131; PECORELLA G., *Circolazione del denaro e riciclaggio*, cit., p. 1232 s.
[106] ZANCHETTI M., *Il riciclaggio di denaro*, cit., p. 361.
[107] *Ibid*., p. 366.
[108] Cass. pen., sez. I, sentenza 23 luglio 2015, n.32491; Cass. pen., sez. II, sentenza 23 febbraio 2005, n. 13448; Cass. pen., sez. II, sentenza 14 ottobre 2003, n. 47088.
[109] ZANCHETTI M., *Il riciclaggio di denaro*, cit., p. 363.
[110] MANES V., *Il riciclaggio dei proventi illeciti*, cit., p. 54.
[111] SEMINARA S., *I soggetti attivi del reato di riciclaggio*, cit., p. 239.

2021, n. 195, di recepimento della direttiva 2018/1673/UE, anche da una contravvenzione. Per questo motivo, il legislatore italiano ha comprensibilmente scelto di non allargare ulteriormente l'ambito applicativo del reato di riciclaggio e di limitarsi a modificare le pene previste per il reato di ricettazione, in modo da adeguarle a quelle previste dalla direttiva. Tale intervento non appare in contrasto con la normativa europea, dato che quest'ultima si limita a prevedere l'obbligo di incriminare le condotte ivi descritte, senza imporre al legislatore di punirle quale riciclaggio invece che ricettazione. Per alcuni il reato di ricettazione ricomprende integralmente le condotte descritte dall'art. 3 par. 1 lett. c) della direttiva 1673/2018/UE[112]. A tal proposito, va osservato che la condotta di acquisto è espressamente menzionata nell'art. 648 c.p., mentre per quanto riguarda il possesso, sebbene non espressamente menzionato, la giurisprudenza della Suprema Corte ritiene integri il delitto di ricettazione la condotta di colui che sia sorpreso nel possesso di un bene di illecita provenienza, senza essere in grado di fornire plausibile giustificazione, qualora, per il luogo e le modalità di occultamento dello stesso bene, possa ritenersene la provenienza illecita[113]. Si evidenzia, però, che la stessa giurisprudenza pacificamente esclude che possa rispondere di ricettazione colui che si limiti a fare uso del bene unitamente agli autori del reato, seppure nella consapevolezza della illecita provenienza. In particolare, si osserva che da questa sola e successiva condotta non si può desumere l'esistenza di una compartecipazione quanto meno d'ordine morale, atteso che il reato di ricettazione ha natura istantanea e non è ipotizzabile una compartecipazione morale per adesione psicologica ad un fatto criminoso da altri commesso[114]. Ad oggi, quindi, l'utilizzazione di beni di provenienza illecita non rientra tra le condotte sanzionate né del riciclaggio, né della ricettazione. Nonostante la non piena conformità alla direttiva, non si ritiene però di dover biasimare il nostro legislatore per non essere intervenuto a punirla. Come si esaminerà meglio nel prosieguo (v. *infra*, cap. V, par. 8), quei Paesi europei che hanno effettivamente inserito anche il possesso e l'uso di beni di provenienza illecita tra le condotte sanzionate a titolo di riciclaggio, hanno dilatato in modo eccessivo l'ambito applicativo della fattispecie, con conseguenti problemi di offensività e proporzionalità della norma penale. Nonostante ciò, trattandosi di direttiva

[112] MORABITO M.A., *Lo schema di decreto legislativo per l'attuazione della direttiva UE 2018/1673*, cit., p. 5.

[113] Cass. pen., sez. II, sentenza 3 novembre 2021, n. 43532; Cass. pen., sez. II, sentenza 18 marzo 2009, n. 26063. Giustamente critico in merito a quest'interpretazione data dalla giurisprudenza è ZANCHETTI M., voce *Ricettazione*, in *Dig. disc. pen.*, vol. XIX, Torino, 1997, p. 174 ss., p. 178, il quale sottolinea che in questo modo si confonde indebitamente la condotta di ricezione con quella del possesso, quando, invece, le due vanno tenute distinte, dato che la prima incrimina solo l'atto di acquisizione del possesso della cosa.

[114] In tal senso v. Cass. pen., sez. V, sentenza 24 settembre 2014, n. 42911; Cass. pen., sez. II, sentenza 5 dicembre 2013, n. 51424; Cass. pen., sez. II, sentenza 13 aprile 2011, n. 23395.

europea, in caso di apertura di una procedura di infrazione per errato recepimento della direttiva europea, il nostro legislatore dovrà necessariamente conformarsi al dettato normativo sovranazionale. L'unica soluzione soddisfacente sarebbe un passo indietro da parte dello stesso legislatore europeo che, preso atto dell'eccessiva ampiezza del novero di condotte previsto dall'art. 3 della menzionata direttiva e anche alla luce dell'esperienza degli altri legislatori europei, potrebbe provvedere ad eliminare l'obbligo per i legislatori europei di punire il possesso e l'utilizzo di beni di illecita provenienza.

Il riciclaggio è, dunque, reato istantaneo, che si consuma con il compimento dell'operazione riciclatoria[115]. Per quanto riguarda la configurabilità del tentativo, abbandonata la configurazione di reato a consumazione anticipata a seguito delle riforme cui è stato soggetto l'art. 648-*bis* c.p., la giurisprudenza della Cassazione lo ritiene astrattamente configurabile per quei casi nei quali l'azione non si è compiuta, perché non è stato possibile eseguire l'operazione[116].

Il riciclaggio è un reato di pericolo concreto[117]. Pertanto, il giudice ha l'obbligo di verificare che l'azione sia realmente idonea ad ostacolare l'individuazione dell'origine del bene. A tal proposito, la giurisprudenza esclude che per la sussistenza del reato sia necessario che la condotta sia volta ad impedire in modo definitivo l'individuazione della provenienza delittuosa dei beni, ma ritiene sia sufficiente che l'accertamento della provenienza del denaro, beni o altre utilità sia resa più difficile[118]. Inoltre, non è necessario che l'origine del bene sia anche effettivamente occultata, ma è sufficiente che la sua individuazione sia resa più ardua[119]. A tal proposito, si ritiene irrilevante che l'operazione sia tracciabile, perché il trasferimento a terzi del denaro provento di reato costituisce comunque condotta idonea ad ostacolarne l'individuazione[120]. Tale principio viene in linea di massima condiviso dalla dottrina, anche se però vi è chi richiama l'attenzione sul rischio che vengano fatti accertamenti meramente simbolici, dato che qualsiasi operazione, dunque anche il mero versamento del denaro su un conto corrente bancario, è potenzialmente idonea a complicare l'attività investigativa[121]. Va tenuto presente che, data la presenza dell'inciso sopra esaminato, la norma in questione non sanziona genericamente l'ostacolo alle indagini,

[115] ACQUAROLI R., *Il riciclaggio*, cit., p. 924.
[116] Cass. pen., sez. I, sentenza 22 febbraio 2022, n. 22437; Cass. pen., sez. II, sentenza 11 dicembre 2014, n. 1960; Cass. pen., sez. V, sentenza 14 gennaio 2010, n. 17694.
[117] DELL'OSSO A.M., *Sub art. 648-bis c.p.*, cit., p. 2323.
[118] Cass. pen., sez. II, sentenza 25 gennaio 2022, n. 2868; Cass. pen., sez. V, sentenza 17 aprile 2018, n. 21925.
[119] Cass. pen., sez. II, sentenza 9 marzo 2015, n. 26208.
[120] Cass. pen., sez. II, sentenza 24 maggio 2019, n. 36121; Cass. pen., sez. II, sentenza 21 settembre 2016, n. 46319.
[121] DELL'OSSO A.M., *Riciclaggio Di Proventi Illeciti*, cit., p. 111.

perché il comportamento deve concretarsi in un ostacolo all'identificazione della provenienza delittuosa dei beni[122].

Alcuni autori ritengono che anche l'acquisto e il trasferimento di criptovalute possa costituire condotta atta ad ostacolare il denaro o le altre utilità di provenienza illecita, sia nei casi in cui le monete rappresentino strumenti di pagamento, sia ove assumano una valenza puramente "speculativa"[123]. Effettivamente in questo caso il reo non si limita a depositare delle somme di denaro, ma le sostituisce con altri beni, in questo caso criptovalute, condotta idonea ad ostacolare l'individuazione della provenienza dei beni, per cui si concorda con tale tesi e si ritiene che tale condotta possa integrare gli estremi del reato in esame. A tal proposito, si può anche evidenziare che non esiste un vero e proprio mercato regolamentato delle criptovalute, per cui è possibile acquistarle anche su siti illegali di *exchange*, che spesso svolgono anche il servizio volto a "confondere" la catena *blockchain* in modo da ostacolare l'individuazione della transazione. Inoltre, le criptovalute possono essere trasferite e conservate in modo anonimo, cosa che costituisce sicuro ostacolo all'identificazione della loro provenienza.

Il riciclaggio è un reato a soggettività ristretta[124], per cui non può rispondere di riciclaggio chi ha partecipato al reato dal quale provengono le attività illecite. La norma, infatti, espressamente esclude la punibilità a titolo di riciclaggio del concorrente nel reato presupposto. L'ambiguità dell'espressione "fuori dai casi di concorso nel reato" ha però dato adito a diverse incertezze interpretative, in particolare con riferimento al suo inquadramento sistematico. In passato in giurisprudenza è stata qualificata come clausola di sussidiarietà espressa[125]. A tale tesi, però si può obiettare che in realtà i fatti storici sanzionati sono diversi, per cui tra le norme non vi può essere sussidiarietà[126]. Per alcuni autori, invece, si tratterebbe di una causa di non punibilità, per cui il legislatore avrebbe ritenuto di evitare l'applicazione congiunta del reato presupposto e dell'art. 648-*bis* c.p. per ragioni di opportunità, al fine di contenere la risposta sanzionatoria complessiva[127]. La tesi più diffusa, però, qualifica i fatti di riciclaggio come postfatti non punibili del reato presupposto, in modo da evitare una duplicazione sanzionatoria per un fatto che rappresenta l'evoluzione di quello commesso[128].

---

[122] ZANCHETTI M., *Il riciclaggio di denaro,* cit., p. 368.
[123] PARODI C., *Tecnologia blockchain, bitcoin e riciclaggio: il futuro è adesso*, in *il penalista,* 14 maggio 2018, disponibile *online* al sito ilpenalista.it.
[124] LONGOBARDO C., *Riciclaggio,* in S. Fiore (a cura di), *I reati contro il patrimonio,* 2010, Torino, p. 819 ss., p. 843; ACQUAROLI R., *Il riciclaggio,* cit., p. 907.
[125] Cass. pen., sez. II, sentenza 6 novembre 2009, n. 47375.
[126] DELL'OSSO A.M., *Riciclaggio Di Proventi Illeciti*, cit., p. 88.
[127] SEMINARA S., *I soggetti attivi del reato di riciclaggio,* cit., p. 236.
[128] ZANCHETTI M., *Il riciclaggio di denaro,* cit., p. 352.

Sul punto sono intervenute le Sezioni Unite della Cassazione, le quali hanno preso atto della difficoltà di inquadramento della clausola di riserva in questione ed hanno ritenuto che essa costituisca una deroga al concorso di reati, che trova la sua ragione di essere nella valutazione, tipizzata dal legislatore, di ritenere l'intero disvalore dei fatti ricompreso nella punibilità del solo delitto presupposto[129].

Ancora più complessa si rivela l'adozione di un criterio per identificare il confine tra riciclaggio e concorso nel reato presupposto, cosa che, come si esaminerà meglio nel prosieguo (v. *infra*, par. 4), assume notevole rilievo proprio con riferimento alle condotte poste in essere nel *web*. Per un primo orientamento la condotta è punibile a titolo di concorso solo se l'accordo finalizzato alla successiva attività di riciclaggio è stato raggiunto prima della commissione del reato presupposto[130]. In questo modo l'esenzione dal riciclaggio sarebbe limitata a chi abbia contribuito alla realizzazione del reato presupposto occupandosi della ripulitura dei proventi illeciti. Tale tesi è però apparsa troppo restrittiva, per cui, secondo l'opinione maggioritaria, per distinguere i casi di riciclaggio da quelli di concorso nel reato presupposto si deve seguire il medesimo criterio utilizzato per la ricettazione. Dunque, ogni contributo che sia causale per il reato presupposto costituisce concorso, a prescindere da un rigido criterio temporale[131]. Pertanto, più che la dislocazione nel tempo rileva l'idoneità del *pactum sceleris* a determinare o rafforzare il proposito criminale negli autori del fatto[132]. Tale criterio ha trovato seguito anche in giurisprudenza[133]. Nel concreto, però, si rivela difficoltoso determinare se una certa condotta debba essere punita a titolo di concorso nel reato presupposto o come fatto di riciclaggio.

Per quanto riguarda l'elemento soggettivo, il riciclaggio è punito unicamente a titolo di dolo. L'Italia, dunque, non fa parte di quel gruppo di Paesi che hanno introdotto fattispecie colpose di riciclaggio (tra cui, come si esaminerà nel prosieguo, Spagna e Germania). Si assiste, pertanto, al paradosso per cui le condotte di minor disvalore sanzionate dalla ricettazione, ovvero l'acquisto e la ricezione di beni di provenienza illecita, sono punite anche a titolo di colpa dalla contravvenzione di incauto acquisto di cui all'art. 712 c.p., mentre così non avviene per le condotte più gravi punite a titolo di riciclaggio.

[129] Cass. pen., sez. un., sentenza 13 giugno 2014, n. 25191.
[130] FAIELLA S., *Riciclaggio e crimine organizzato transnazionale*, cit., p. 289.
[131] ZANCHETTI M., *Il riciclaggio di denaro*, cit., p. 355; DELL'OSSO A.M., *Riciclaggio Di Proventi Illeciti*, cit., p. 85.
[132] ACQUAROLI R., *Il riciclaggio*, cit., p. 908.
[133] Cass. pen., sez. V, sentenza 10 gennaio 2007, n. 8432.

Il dolo di riciclaggio è generico. Il riferimento al dolo specifico, infatti, è stato eliminato sin dalla riforma del 1990 allo scopo di conferire alla norma maggiore semplicità e chiarezza[134]. Pertanto, ai fini del dolo di riciclaggio è sufficiente avere la consapevolezza e la volontà che i vantaggi siano portati nei settori economici o finanziari sopra citati e la consapevolezza generale che tali vantaggi provengono da qualche precedente reato. Non è, invece, necessario che l'autore del reato agisca con l'intento specifico di arricchire o trarre profitto per sé o per l'autore del reato presupposto[135].

Tradizionalmente dibattuta è la configurabilità del riciclaggio a titolo di dolo eventuale. Alcuni autori la escludono, evidenziando che per la punibilità a titolo di dolo eventuale bisognerebbe provare l'esistenza di un *quid pluris* rispetto al semplice dubbio sul presupposto del reato, dato che non è mai prova sufficiente del dolo il fatto che il soggetto "avrebbe dovuto sapere" che i beni costituivano proventi di reato. Poiché tale prova è troppo incerta, non si può che escludere la compatibilità del dolo eventuale[136]. Tale obiezione, però, a ben vedere non esclude in astratto la compatibilità del riciclaggio col dolo eventuale, bensì evidenzia le difficoltà dell'accertamento in concreto[137]. Dunque, in assenza di indicazioni di segno contrario, sia una parte consistente della dottrina[138] che la giurisprudenza[139], ritengono che il dolo di riciclaggio possa essere anche eventuale. Come si esaminerà meglio nel prosieguo, però, ammettere la rilevanza del dolo eventuale pone diversi problemi.

Infine, è prevista una circostanza aggravante speciale per il fatto "commesso nell'esercizio di un'attività professionale", che stigmatizza il maggior disvalore del fatto commesso da soggetti che per la loro attività possono agevolare la surrogazione di proventi illeciti[140]. Per quanto riguarda la professionalità dell'attività svolta, non è richiesto che il soggetto sia iscritto in un apposito albo o che l'attività richieda una speciale abilitazione, ma è sufficiente lo svolgimento di qualunque attività economica o finanziaria diretta a creare nuovi beni e servizi o allo scambio e distribuzione di beni nel mercato del consumo[141]. Inoltre, come già sopra accennato, è prevista una circostanza aggravante speciale per il caso

[134] ZANCHETTI M., *Il riciclaggio di denaro*, cit., p. 385.
[135] Cass. pen., sez. II, sentenza 11 gennaio 2011, n. 546; Cass. pen., sez. VI, sentenza 18 dicembre 2007, n. 16980; Cass. pen., sez. IV, sentenza 15 febbraio 2007, n. 6350; Cass. pen., sez. II, sentenza 12 aprile 2005, n. 13448.
[136] ZANCHETTI M., *Il riciclaggio di denaro*, cit., p. 435.
[137] DELL'OSSO A.M., *Sub art. 648-bis c.p.*, cit., p. 2323.
[138] FLICK G.M., *La repressione del riciclaggio ed il controllo dell'intermediazione finanziaria*, cit., p. 1256; PECORELLA G., *Circolazione del denaro e riciclaggio*, cit., p. 1244.
[139] Cass. pen., sez. II, sentenza 7 ottobre 2016, n. 52241; Cass. pen., sez. V, sentenza 17 aprile 2018, n. 21925.
[140] INSOLERA G., *Diritto penale e criminalità organizzata*, cit., p. 150.
[141] Cass. pen., sez. II, sentenza 6 dicembre 2016, n. 3026.

in cui il denaro, i beni o le altre utilità provengono da delitto per il quale è stabilita la pena della reclusione inferiore nel massimo a cinque anni.

3.2. Impiego di denaro, beni o utilità di provenienza illecita

Come sopra evidenziato, a comporre il quadro normativo delle fattispecie contro il riciclaggio vi è anche l'art. 648-*ter* c.p., intitolato impiego di denaro, beni o utilità di provenienza illecita. La fattispecie in esame è stata introdotta dalla l. n. 55/1990 ed è stata subito dopo modificata con la legge di ratifica della Convenzione di Strasburgo del 1993, andando a costituire il completamento del delitto di riciclaggio. Alcuni autori, invece, hanno negato che vi fosse l'esigenza di introdurre una norma *ad hoc* di questo tenore, dato che l'ambito applicativo del riciclaggio è particolarmente ampio[142]. Per altri, invece, l'autonoma incriminazione delle condotte di impiego ha la sua ragion d'essere, dato che l'intervento che avrebbero potuto offrire le altre fattispecie sarebbe stato inappagante[143]. Si concorda, però, con coloro che ritengono che essa costituisca l'esempio di una fattispecie penale simbolica, apparentemente rigorosa, ma di fatto inutilizzabile[144]. Ne è prova lo scarsissimo numero di pronunce giurisprudenziali in merito a più di trent'anni dalla sua introduzione. La norma, infatti, si apre con la clausola di sussidiarietà espressa "fuori dei casi di concorso nel reato e dei casi previsti dagli artt. 648 e 648-*bis* c.p.", sussidiarietà che finisce col privare la fattispecie di significato pratico riducendola ad una norma simbolica[145].

La clausola di riserva è stata oggetto di critiche perché finisce per "paralizzare" l'applicazione della norma riferita all'aspetto più grave e socialmente più dannoso del riciclaggio[146]. In base a tale clausola di sussidiarietà, infatti, non può essere punito chi ha già commesso il reato presupposto di ricettazione ex art. 648 c.p. o di riciclaggio ex art. 648-*bis* c.p. Tuttavia, risulta difficile trovare uno spazio di autonomia per l'art. 648-*ter* rispetto all'art. 648-*bis* c.p. La sussidiarietà rispetto all'art. 648 c.p., infatti, appare chiudere i residui ambiti di applicabilità della fattispecie, dato che non sembra possano configurarsi ipotesi di "impiego" di proventi criminosi che non presuppongano una ricettazione, salvo comportamenti in cui difetti il dolo specifico di profitto o comportamenti che non implichino

[142] ZANCHETTI M., *Il riciclaggio di denaro*, cit., p. 451.
[143] DELL'OSSO A.M., *Riciclaggio Di Proventi Illeciti*, cit., p. 143.
[144] MOCCIA S., *Impiego di capitali illeciti e riciclaggio*, cit., p. 451.
[145] INSOLERA G., *Diritto penale e criminalità organizzata*, cit., p. 147; ZANCHETTI M., *Il riciclaggio di denaro*, cit., p. 452.
[146] MOCCIA S., *Effettività e normativa antiriciclaggio*, in E. Palombi (a cura di), *Il riciclaggio dei proventi illeciti. Tra politica criminale e diritto vigente*, Napoli, 1996, p. 303 ss., p. 305; MANES V., *Il riciclaggio dei proventi illeciti*, cit., p. 62 s.

alcun contatto con l'oggetto materiale del reato, né alcun trasferimento di tale oggetto dal concorrente nel reato base a terze persone[147]. Dato che, però, appare difficile ipotizzare un reimpiego non preceduto dalla ricettazione, nel caso in cui sussista il fine di trarre profitto si applica l'art. 648 c.p., per cui vi è un'irrazionale e più blanda risposta sanzionatoria[148]. Il reato in questione, dunque, trova scarsa applicazione nell'ambito della criminalità generale o organizzata, poiché un gran numero di casi di reimpiego rientra in questa clausola di sussidiarietà.

Anche in questo caso si tratta di reato a soggettività ristretta, dato che l'autore non può essere chi ha commesso o concorso a commettere il reato presupposto[149]. Per quanto riguarda il bene giuridico tutelato, per alcuni autori l'art. 648-*ter* c.p. tutelerebbe in via prioritaria l'ordine economico, che potrebbe essere turbato dall'immissione nel mercato di beni e soprattutto di capitali di provenienza delittuosa, alterando la libera concorrenza[150]. Per altri, invece, essa mira a salvaguardare non il bene giuridico dell'efficiente amministrazione della giustizia, ma quello del risparmio/investimento[151]. Per la giurisprudenza si tratterebbe anche in questo caso di reato plurioffensivo, posto a tutela sia dell'ordine economico che del patrimonio[152].

Anche la fattispecie di impiego di denaro, beni o utilità di provenienza illecita è costruita come reato accessorio, perché presuppone l'integrazione di un altro reato da parte di soggetti diversi dall'autore[153]. Analogamente al riciclaggio, neppure in tale fattispecie è presente un catalogo di reati presupposto. Anche qui, però, vi è una circostanza attenuante speciale per il caso in cui il reato presupposto sia costituito da un delitto per il quale è stabilita la pena della reclusione inferiore nel massimo a 5 anni[154]. A differenza che per l'art. 648-*bis* c.p., nell'art. 648-*ter* c.p. manca sin dall'origine la precisazione che il delitto presupposto deve essere non colposo. Anche questo reato è stato modificato dal d.lgs. 8 novembre 2021, n. 195, per cui il novero dei reati presupposto è stato ulteriormente esteso alle contravvenzioni punite con l'arresto superiore nel massimo a un anno o nel minimo a sei mesi[155]. Pure in questo caso la punibilità ai sensi dell'art. 648-*ter* c.p. non è esclusa

[147] ZANCHETTI M., *Il riciclaggio di denaro*, cit., p. 452 s.
[148] INSOLERA G., *Diritto penale e criminalità organizzata*, cit., p. 147.
[149] DELL'OSSO A.M., *Riciclaggio Di Proventi Illeciti*, cit., p. 146.
[150] FIANDACA G., MUSCO E., *Diritto penale. PS*, cit., p. 271.
[151] ZANCHETTI M., *Il riciclaggio di denaro*, cit., p. 455.
[152] Cass. pen., sez. IV, sentenza 23 marzo 2000, n. 6534.
[153] ACQUAROLI R., *Il reimpiego di capitali illeciti*, in C. Piergallini, F. Viganò, M. Vizzardi, A. Verri (a cura di), *I delitti contro la persona*, cit., p. 937 ss., p. 937.
[154] AMATO G., *Il riciclaggio del denaro "sporco"*, cit., p. 140.
[155] PESTELLI G., *Riflessioni critiche sulla riforma dei reati di ricettazione*, cit., p. 54.

nell'ipotesi in cui manchi una condizione di procedibilità per il reato presupposto o se l'autore di questi sia non imputabile o non punibile[156].

Gli oggetti del reato di cui all'art. 648-*ter* c.p. sono gli stessi di cui al reato di riciclaggio, ovvero denaro, beni o altre utilità. Anche in questo caso, analogamente a quanto scritto sopra per il reato di riciclaggio, si ritiene possano costituire oggetto del reato in esame anche le criptovalute. Il riferimento a "beni o altre utilità" al plurale viene interpretato nel senso di ritenere sussistente un unico reato anche in caso di molteplici attività d'impiego, per cui in quest'ultimo caso si tratterebbe di un reato eventualmente abituale[157].

Il reato di cui all'art. 648-*ter* c.p. punisce la condotta di impiego dei proventi in attività economiche o finanziarie. Si ha "impiego" quando si adoperano denaro, beni o altre utilità per la produzione o il commercio di beni o servizi, per la circolazione di denaro o titoli che li rappresentano, per le intermediazioni e in generale per qualunque altra destinazione avente un interesse economico[158]. Per alcuni autori la condotta di impiego è suscettibile di una lettura più ampia che la diversifica dal concetto di investimento, per cui è configurabile in qualunque uso dei proventi illeciti, a prescindere da intenti od obiettivi speculativi[159]. Altri, invece, ritengono che l'impiego non possa essere inteso come sinonimo di utilizzo, pena un'eccessiva dilatazione dell'ambito applicativo della fattispecie, bensì come investimento, per cui dev'essere comunque valorizzato il fine di profitto[160].

La norma stessa non contiene ulteriori definizioni o riferimenti per l'interpretazione degli elementi di "attività economiche" o "attività finanziarie". Tuttavia, si può affermare che le attività economiche si riferiscono principalmente alla produzione, al commercio e ad altri servizi, mentre l'economia finanziaria comprende il commercio di denaro e di titoli, nonché la gestione e l'incremento delle attività finanziarie[161]. Si tratta, quindi, del complesso delle attività idonee a generare profitti, che sono quelle potenzialmente produttive di ricchezza[162]. Per la giurisprudenza la nozione di attività economica o finanziaria è desumibile dagli artt. 2082, 2135, 2195 c.c. e fa riferimento non solo all'attività produttiva in senso stretto, ossia a quella diretta a creare nuovi beni o servizi, ma anche all'attività di scambio e di distribuzione dei beni nel mercato del consumo, nonché ad ogni altra attività che possa rientrare in una di quelle elencate nelle sopra menzionate norme del codice

[156] ACQUAROLI R., *Il reimpiego di capitali illeciti*, cit., p. 939.
[157] ZANCHETTI M., *Il riciclaggio di denaro,* cit., p. 456.
[158] PECORELLA G., *Circolazione del denaro e riciclaggio,* cit., p. 1236.
[159] INSOLERA G., *Diritto penale e criminalità organizzata*, cit., p. 152.
[160] DELL'OSSO A.M., *Riciclaggio Di Proventi Illeciti*, cit., p. 148.
[161] PECORELLA G., *Circolazione del denaro e riciclaggio,* cit., p. 1240.
[162] ZANCHETTI M., *Il riciclaggio di denaro,* cit., p. 456.

civile[163]. Queste attività possono essere svolte anche nel *cyberspace*[164]. In relazione all'impiego del denaro sporco, la norma non specifica se le attività economiche o finanziarie debbano essere lecite o illecite. In giurisprudenza si è sostenuta la rilevanza di condotte di impiego in attività illecite[165], anche se in dottrina non manca chi rileva che la finalità della norma è quella di salvaguardare i mercati finanziari regolari dalle contaminazioni di capitali illeciti, per cui appare logico ritenere che le attività economiche e finanziarie nelle quali confluiscono gli impieghi debbano avere carattere lecito[166].

Il reato di cui all'art. 648-*ter* c.p. è reato istantaneo, che si consuma nel momento e nel luogo dell'impiego[167].

A differenza che nell'art. 648-*bis* c.p., qui manca la menzione "in modo da ostacolare l'identificazione della provenienza delittuosa del bene". La norma, dunque, punisce anche gli atti con i quali le utilità vengono attivamente reimmesse nel ciclo economico e investite, indipendentemente dal fatto che tali atti siano idonei a dissimulare la provenienza delittuosa dei beni economici[168]. L'ambito di applicazione del reato è quindi più ampio di quello del riciclaggio di cui all'art. 648-*bis* c.p., dato che è sufficiente che i beni siano in qualche modo introdotti in attività economiche o affluiscano nel mercato finanziario, senza che ciò debba anche rendere più difficile l'identificazione dell'origine illecita degli stessi[169]. Pertanto, può essere classificato come un reato di pericolo astratto[170].

La differenza tra il riciclaggio di denaro e l'impiego dello stesso non è facile da individuare. Alcuni autori sostengono che il reato di cui all'art. 648-*ter* c.p. prevede non solo di rendere più difficile l'accertamento della provenienza delittuosa del denaro, ma anche di occultare la provenienza delittuosa mediante attività economiche o finanziarie[171]. La differenza tra i due reati, dunque, interverrebbe già sul piano della condotta e sarebbe riferita all'elemento oggettivo[172]. La giurisprudenza sostiene che la differenza tra i due reati risiede invece nell'elemento soggettivo, perché nell'art. 648-*ter* c.p. l'autore deve agire in modo

[163] Cass. pen., sez. II, sentenza 9 settembre 2018, n. 38422; Cass. pen., sez. II, sentenza 14 luglio 2016, n. 33076; Cass. pen., sez. II, sentenza 4 febbraio 2014, n. 5546.
[164] PICOTTI L., *Profili penali del cyberlaundering*, cit., p. 609.
[165] Cass. pen., sez. II, sentenza 25 febbraio 2014, n. 9026.
[166] DELL'OSSO A.M., *Riciclaggio Di Proventi Illeciti*, cit., p. 149.
[167] DELL´OSSO A.M., *Sub art. 648-ter c.p.*, cit., p. 2327.
[168] LONGOBARDO C., *Impiego di denaro, beni o utilità di provenienza illecita*, in S. Fiore (a cura di), *I reati contro il patrimonio*, Torino, 2010, p. 884 ss., p. 886.
[169] DELL'OSSO A.M., *Sub art. 648-ter c.p.*, cit., p. 2327.
[170] *Ibidem*
[171] PLANTAMURA V., *Il cybericiclaggio*, cit., p. 861.
[172] ZANCHETTI M., *Il riciclaggio di denaro*, cit., p. 452; DELL'OSSO A.M., *Sub art. 648-ter c.p.*, cit., p. 2328.

definitivo con la specifica intenzione di trarre profitto da attività economiche o finanziarie[173]. In altre pronunce, però, si è sostenuto che la distinzione sarebbe da individuare utilizzando il criterio dell'unicità o pluralità di azioni e determinazioni volitive. Pertanto, commette impiego chi riceve o manipola utilità lecite per impiegarle in attività economiche, avendo sin dal principio programmato di destinarle in tale modo[174].

Per quanto riguarda l'elemento soggettivo, pure in questo caso è sufficiente il dolo generico, che consiste nella rappresentazione dell'origine delittuosa dell'utilità e nella consapevole volontà di investirla in attività economiche o finanziarie[175]. È da escludere, dunque, che la norma richieda una specifica finalità[176]. Inoltre, anche nel caso dell'art. 648-*ter* c.p. si ritiene configurabile il dolo eventuale[177].

Infine, anche quest'ultimo reato prevede una circostanza aggravante per il fatto commesso nell'esercizio di un'attività professionale, sulla quale ci si richiama a quanto già esposto in merito all'identica circostanza contenuta nell'art. 648-*bis* c.p.

3.3 L'autoriciclaggio

Come sopra accennato, oggi nel nostro ordinamento anche il riciclaggio commesso dall'autore o dal concorrente nel reato presupposto è penalmente sanzionato. La punibilità dell'autoriciclaggio è stata introdotta nel nostro ordinamento dall'art. 3, co. 3, L. 15 dicembre 2014, n. 186, attraverso la quale è stato introdotto nel codice penale l'art. 648-*ter*.1. Tale legge aveva lo scopo di regolamentare la c.d. *voluntary disclosure*, ovvero la procedura di collaborazione volontaria con la quale il contribuente infedele può autodenunciarsi al fisco e sanare così le violazioni commesse[178]. Alcuni autori, dunque, hanno ipotizzato che l'introduzione del reato in esame fosse destinata ad incentivare ulteriormente il ricorso alla procedura di emersione volontaria dei capitali indebitamente detenuti all'estero, poiché la minaccia della sanzione penale avrebbe potuto spingere i contribuenti infedeli ad autodenunciarsi per andare esenti da pena[179]. Altri, però, ritengono che la normativa sulla *voluntary disclosure* fosse solo un'occasione per rivedere il tema della

[173] Cass. pen., sez. III, sentenza 14 luglio 2016, n. 33076; Cass. pen., Sez. II, 10/01/2003, n. 18103.
[174] Cass. pen., sez. II, sentenza 15 aprile 2016, n. 30429; Cass. pen., sez. II, sentenza 11 aprile 2013, n. 16432.
[175] DELL'OSSO A.M., *Riciclaggio Di Proventi Illeciti*, cit., p. 149.
[176] Cass. pen., sez. II, sentenza 8 ottobre 2019, n. 43387.
[177] DELL´OSSO A.M., *Sub art. 648-ter c.p.*, cit., p. 2327.
[178] INGRASSIA A., *Le (caleidoscopiche) ricadute penalistiche della procedura di* voluntary disclosure*: causa sopravvenuta di non punibilità, autodenuncia e condotta penalmente rilevante*, in *Riv. trim. dir. pen. cont*., 2015, n. 2, p. 127 ss., p. 128.
[179] CAVALLINI S, TROYER L., *Apocalittici o integrati? Il nuovo reato di autoriciclaggio: ragionevoli sentieri ermeneutici all'ombra del "vicino ingombrante"*, in *Riv. trim. dir. pen. cont*., 2015, n. 1, p. 95 ss., p. 107.

punibilità dell'autoriciclaggio, da anni oggetto di dibattito, dato che essa si poneva come istituto di carattere temporaneo, mentre il reato di autoriciclaggio era destinato a rimanere all'interno del codice penale[180]. Come sopra evidenziato, le fonti internazionali prevedevano e auspicavano la criminalizzazione del fenomeno, così come una parte della dottrina[181]. Oggi, peraltro, la punibilità del riciclaggio da parte dell'autore del reato presupposto è espressamente imposta dal legislatore europeo all'art. 3 par. 5 della direttiva 2018/1673/UE sulla lotta al riciclaggio mediante il diritto penale.

Il privilegio di autoriciclaggio dava all'autore del reato presupposto un vantaggio ingiusto, dato che quest'ultimo ben avrebbe potuto essere punito meno gravemente del riciclaggio[182]. Per cui, ben poteva accadere che l'autore del reato presupposto che impiegava i profitti in attività economiche rispondesse di una pena più lieve rispetto al terzo estraneo che compiva la medesima attività. Non sono però mancate in dottrina voci critiche in merito all'introduzione del reato in esame, per la potenziale violazione dei principi del *ne bis in idem*, nonché del *nemo tenetur se detegere*[183].

Il nostro legislatore, a differenza di altri legislatori europei (v. *infra*, cap. V, par. 9), ha preferito introdurre una nuova fattispecie *ad hoc* per punire l'autoriciclaggio, al posto di eliminare la clausola di riserva di cui all'art. 648-*bis* c.p. Tale scelta è assolutamente condivisibile, dato che, come osservato[184], la criminalizzazione dell'autoriciclaggio richiede particolari cautele poiché si rischia di sanzionare fatti che rappresentano la necessaria evoluzione del reato presupposto o che rientrano nella strategia difensiva per evitare la condanna. L'eliminazione *sic et simpliciter* di tale clausola, infatti, avrebbe determinato una notevole espansione della punibilità[185], come, peraltro, come si esaminerà meglio nel prosieguo, è avvenuto nell'ordinamento spagnolo.

---

[180] DELL'OSSO A.M., *Sub art. 648-ter.1*, in G. Forti, S. Seminara, G. Zuccalà (a cura di), *Commentario breve al codice penale*, 2016, Padova, p. 2329 ss., p. 2329.

[181] Così SEMINARA S., *I soggetti attivi del reato di riciclaggio*, cit., p. 235, secondo cui «*l'elevata offensività delle pene previste dall'art. 648-bis c.p. dovrebbe indurre ad escludere qualsiasi limitazione della cerchia dei possibili soggetti attivi*». Nello stesso senso anche FAIELLA S., *Riciclaggio e crimine organizzato transnazionale*, cit., p. 281 ss.

[182] BRICCHETTI R., *Riciclaggio e auto-riciclaggio*, cit., p. 694.

[183] SGUBBI F., *Il nuovo delitto di "autoriciclaggio": una fonte inesauribile di "effetti perversi" dell'azione legislativa*, in *Dir. pen. cont*. 2015, n. 1, p. 137 ss., p. 137 ss; PIVA D., *Il volto oscuro dell'autoriciclaggio: la fine di privilegi o la violazione di princìpi?*, in *Resp. amm. soc. enti*, 2015, n. 3, p. 59 ss., 62 ss.; CAVALLINI S, TROYER L., *La "clessidra" del riciclaggio ed il privilegio di* self-laundering*: note sparse a margine di ricorrenti, astratti furori del legislatore*, in *Riv. trim. dir. pen. cont*. 2014, n. 2, p. 49 ss., p. 62 ss.; DELL'OSSO A.M., *Riciclaggio Di Proventi Illeciti*, cit., p.

[184] DELL'OSSO A.M., *Il reato di autoriciclaggio: la politica criminale cede il passo a esigenze mediatiche e investigative*, in *Riv. it. dir. proc. pen*., 2015, n. 2, p. 796 ss., p. 803.

[185] CAVALLINI S, TROYER L., *La "clessidra" del riciclaggio ed il privilegio di* self-laundering, cit., p. 62; MANES V., *Il riciclaggio dei proventi illeciti*, cit., p. 75.

Per quanto riguarda il bene giuridico tutelato dall'art. 648-*ter*.1 c.p., vi è chi ritiene che esso coincida con la tutela dell'ordine economico[186]. Si evidenzia, però, che il disvalore delle condotte è polarizzato sull'attitudine delle stesse a costituire un ostacolo concreto all'identificazione della provenienza delittuosa dei beni, per cui in realtà oggetto di tutela sarebbe l'amministrazione della giustizia[187]. Altri ancora ritengono che anch'esso, analogamente al riciclaggio, sia reato plurioffensivo, in cui gli interessi giuridici tutelati sono il patrimonio, l'amministrazione della giustizia e l'ordine economico e finanziario[188].

Come previsto dalla norma, autore del reato di autoriciclaggio può essere soltanto colui che ha commesso o ha concorso a commettere il reato presupposto. Per alcuni autori il reato in questione va inquadrato come reato proprio[189]. Per altri, però, non si tratterebbe solo di un reato proprio, bensì di un reato proprio c.d. esclusivo o di mano propria, nel quale l'esecuzione della condotta tipica dev'essere compiuta direttamente dal soggetto qualificato[190]. A tale ultima tesi è stato obiettato che nei reati di mano propria il disvalore è intimamente connesso all'azione del soggetto titolato, mentre in questo caso la stessa identica condotta commessa da un terzo integra addirittura un reato più grave[191].

La questione non è priva di rilevanza pratica, in specie ai fini della configurabilità del concorso del terzo, estraneo al reato presupposto, nel reato di autoriciclaggio. Infatti, se si aderisce alla tesi secondo cui il fatto tipico deve essere realizzato dal soggetto qualificato, qualora sia il terzo a realizzare l'impiego fornendo un contributo concorsuale causalmente rilevante alla condotta di autoriciclaggio posta in essere dall'*intraneus*, costui non risponderà di concorso in autoriciclaggio, bensì di riciclaggio o reimpiego ex art. 648-*ter* c.p. Sul punto si è espressa la giurisprudenza della Cassazione, ritenendo che qualora il soggetto che non sia concorrente nel reato presupposto ponga in essere la condotta tipica di autoriciclaggio, o

---

[186] MUCCIARELLI F., *Qualche nota sul delitto di autoriciclaggio*, in *Dir. pen. cont*., 2015, n. 1, p. 108 ss., p. 112.
[187] DELL'OSSO A.M., *Riciclaggio Di Proventi Illeciti*, cit., p. 180 s.
[188] PIERGALLINI C., *Autoriciclaggio, concorso di persone e responsabilità dell'ente: un groviglio di problematica ricomposizione*, in *Discrimen*, 2015, p. 539 ss., p. 551; CROCE M., *Cyberlaundering e valute virtuali*, cit., p. 141 s.
[189] DELL'OSSO A.M., *Riciclaggio Di Proventi Illeciti*, cit., p. 183 ss.; BASILE E., *L'autoriciclaggio nel sistema penalistico di contrasto al* money laundering *e il nodo gordiano del concorso di persone*, in *Cass. pen*., 2017, n. 3, p. 1277 ss., p. 1295; SEMINARA S., *Spunti interpretativi sul delitto di autoriciclaggio*, in *Dir. pen. proc*., 2016, n. 12, p. 1631 ss., p. 1639; GULLO A., *Realizzazione plurisoggettiva dell'autoriciclaggio: la Cassazione opta per la differenziazione dei titoli di reato*, in *Dir. Pen. Cont.*, 2018, n. 6, p. 262 ss., p. 265 ss.
[190] MUCCIARELLI F., *Qualche nota sul delitto di autoriciclaggio*, cit., p. 119; PIERGALLINI C., *Autoriciclaggio, concorso di persone e responsabilità dell'ente*, cit., p. 551.
[191] SEMINARA S., *Spunti interpretativi sul delitto di autoriciclaggio*, cit., p. 1647; BASILE E., *L'autoriciclaggio nel sistema penalistico di contrasto al* money laundering *e il nodo gordiano del concorso di persone*, in *Cass. pen*., 2017, n. 3, p. 1277 ss., p. 1295; DELL'OSSO A.M., *Riciclaggio Di Proventi Illeciti*, cit., p. 185.

comunque contribuisca alla realizzazione da parte dell'*intraneus* delle condotte tipizzate dall'art. 648-*ter*.l c.p., risponde necessariamente del reato di riciclaggio ex art. 648-*bis* c.p., ovvero, ricorrendone i presupposti, di quello contemplato dall'art. 648-*ter* c.p., mentre non può configurarsi concorso di persone nel meno grave delitto di autoriciclaggio ex art. 648-*ter*.l c.p., dato che quest'ultima norma prevede e punisce come reato unicamente le condotte poste in essere dal soggetto che abbia commesso o concorso a commettere il reato presupposto, in precedenza non previste e punite come reato[192]. Al contempo, però, ha escluso che possa ancora considerarsi penalmente irrilevante la condotta di colui che abbia preso parte al reato presupposto e che si sia limitato a mettere a disposizione il provento del predetto delitto nelle mani di un terzo perché lo reimpieghi, senza compiere in prima persona la condotta tipica di autoriciclaggio[193].

La questione è estremamente rilevante per quanto riguarda i proventi di reati cibernetici, i quali in alcuni casi vengono appositamente affidati a soggetti terzi ed estranei al reato presupposto proprio per essere ripuliti, mentre in altri casi i cybercriminali si avvalgono dell'intervento di un *financial manager* (v. *infra*, par. 4) per farne perdere le tracce. Seguendo il richiamato principio enunciato dalla Suprema Corte, infatti, i cybercriminali dovrebbero rispondere del reato di autoriciclaggio, mentre i *financial manager* del più grave reato di riciclaggio.

Anche in questo caso reato presupposto può essere qualsiasi delitto e, a seguito del d.lgs. 195/2021, anche le contravvenzioni punite con l'arresto superiore nel massimo a un anno o nel minimo a sei mesi[194]. Gli oggetti del reato, inoltre, sono gli stessi già previsti per gli artt. 648-*bis* e 648-*ter* c.p., ovvero denaro, beni o altre utilità. Data la presenza del richiamo all'ultimo comma dell'art. 648 c.p., pure in questo caso il reato sussiste anche se il soggetto non è imputabile o punibile per il reato presupposto. Tuttavia, il richiamo all'imputabilità appare assai bizzarro, dato che l'autore dell'autoriciclaggio è il medesimo soggetto che ha commesso il reato presupposto.

La condotta sanzionata dalla norma in questione consiste nell'impiego, nella sostituzione o nel trasferimento dei proventi in attività economiche, finanziarie,

---

[192] Cass. pen., sez. II, sentenza 17 gennaio 2018, n. 17235.

[193] *Ibid*.: «*Da questa ineludibile premessa discende […], l'impossibilità di interpretare la normativa allo stato vigente: […]- sia nel senso della perdurante irrilevanza penale della condotta dell'intraneus (ovvero del soggetto che abbia preso parte al delitto presupposto non colposo) che si sia limitato a mettere a disposizione il provento del predetto delitto nelle mani del terzo, perché lo reimpieghi, senza compiere in prima persona la condotta tipica di autoriciclaggio (come risulterebbe necessario ritenere ove si configurasse l'autoriciclaggio come delitto "di mano propria"*)».

[194] PESTELLI G., *Riflessioni critiche sulla riforma dei reati di ricettazione,* cit., p. 50 s.

imprenditoriali o speculative. Essa, dunque, costituisce un ibrido tra quelle sanzionate dalla fattispecie di riciclaggio e da quella di impiego di denaro, beni o utilità di provenienza illecita. Anche in questo caso, analogamente al riciclaggio, si tratta di norma a più fattispecie, per cui la realizzazione di più di una delle condotte sopra descritte integra comunque un solo reato[195]. La disposizione di nuovo conio tipizza e sanziona il comportamento consistente nella re-immissione nel circuito dell'economia legale di beni attraverso modalità in concreto idonee ad ostacolare la identificazione della loro provenienza[196]. Trattasi, dunque, di fatti avulsi alle dinamiche del reato presupposto. Per questo motivo, alcuni autori escludono che la norma in questione contrasti coi principi del *ne bis in idem* e del *nemo tenetur se detegere*[197].

Tra i reati di autoriciclaggio, riciclaggio ed impiego di denaro, beni o utilità di provenienza illecita, pertanto, non esiste una perfetta sovrapponibilità, dato che il reato di autoriciclaggio ha un ambito di applicazione più ristretto rispetto alle altre due fattispecie[198]. Manca, infatti, la clausola di chiusura relativa al compimento di "altre operazioni", presente nel reato di riciclaggio. A tal proposito, la giurisprudenza ha evidenziato che restano escluse dall'ambito applicativo dell'autoriciclaggio quelle operazioni distinte dalla sostituzione e dal trasferimento in attività economiche, finanziarie, imprenditoriali o speculative che siano tali da frapporre ostacoli all'identificazione di denaro e beni di provenienza illecita, operazioni che, invece, rientrano nella fattispecie di riciclaggio[199]. È poi richiesto un ulteriore elemento di illiceità, in quanto gli oggetti del reato devono essere utilizzati attraverso attività economiche, finanziarie, imprenditoriali o speculative.

La fattispecie prevede poi che le condotte in questione siano realizzate "in modo tale da ostacolare concretamente l'identificazione" della provenienza illecita dei beni. Tale clausola consente di delimitare l'ambito applicativo della fattispecie, perché impone di sanzionare non qualsiasi re-immissione nell'economia legale di beni di provenienza delittuosa, ma soltanto quella concretamente idonea ad occultare l'illecita provenienza del bene[200]. L'autoriciclaggio, dunque, è un reato di pericolo concreto, perché la formulazione dell'art. 648-ter.1 c.p. richiede che l'accertamento della provenienza delittuosa dei benefici

[195] DELL'OSSO A.M., *Sub art. 648-ter.1*, cit., p. 2331.
[196] MUCCIARELLI F., *Qualche nota sul delitto di autoriciclaggio*, cit., p. 118.
[197] BASILE E., *L'autoriciclaggio nel sistema penalistico di contrasto al* money laundering *e il nodo gordiano del concorso di persone*, cit., p. 1280 ss.
[198] DELL'OSSO A.M., *Riciclaggio Di Proventi Illeciti*, cit., p. 84.
[199] Cass. pen., sez. II, 11 luglio 2019, n. 41686.
[200] MUCCIARELLI F., *Qualche nota sul delitto di autoriciclaggio*, cit., p. 115.

sia concretamente impedito[201]. In questo caso, il concreto ostacolo non può consistere in un generico rallentamento delle indagini dell'autorità giudiziaria, ma deve estrinsecarsi in un effettivo intralcio alla tracciabilità del denaro[202]. A tal proposito, la giurisprudenza ritiene però che ai fini dell'integrazione del reato in esame non sia necessario che l'agente ponga in essere una condotta di impiego, sostituzione o trasferimento del denaro, beni o altre utilità che comporti un assoluto impedimento alla identificazione della provenienza delittuosa degli stessi, ma sia, invece, sufficiente una qualunque attività, concretamente idonea anche solo ad ostacolare gli accertamenti sulla loro provenienza[203]. A tal fine, è stata ritenuta condotta idonea ad integrare il reato di autoriciclaggio anche quella di colui che abbia utilizzato i proventi delle truffe per l'acquisto di criptovalute tramite una serie di bonifici, ritenendo che l'acquisto di valuta virtuale possa costituire "attività speculativa"[204]. Altrettanto è stato ritenuto per il mero trasferimento di denaro di provenienza delittuosa tramite bonifico da un conto corrente bancario ad altro diversamente intestato[205].

Anche l'autoriciclaggio è reato istantaneo, che si consuma con la commissione di una delle condotte tipiche e, analogamente all'art. 648-*bis* c.p., neanche in questo caso appaiono esservi ostacoli alla configurabilità del tentativo[206].

Per quanto riguarda l'elemento soggettivo, anche in questo caso è sufficiente il dolo generico, per cui è sufficiente che l'autore utilizzi il denaro, i beni o le utilità con la consapevolezza che gli stessi provengono da un reato e impedisca deliberatamente di determinarne l'origine[207].

Nel co. 4 dell'art. 648-*ter*. 1 c.p. è stata inserita una clausola di non punibilità, che esclude la rilevanza penale della condotta nei casi in cui i beni oggetto di autoriciclaggio vengano destinati alla mera utilizzazione o al godimento personale. Una clausola di non punibilità del genere è conforme alle disposizioni di cui alla direttiva 2018/1673/UE, dato che all'art. 3 par. 5 essa menziona tra le condotte di riciclaggio che gli Stati membri devono sanzionare unicamente quelle di cui alle lett. a) e b), escludendo, dunque, l'obbligo del legislatore nazionale di sanzionare penalmente l'acquisto, la detenzione o l'utilizzazione di

[201] DALL'OSSO A.M., *Sub art. 648-ter.1,* cit., p. 2332.
[202] SEMINARA S., *Spunti interpretativi sul delitto di autoriciclaggio*, cit., p. 1644.
[203] Cass. pen., sez. II, sentenza 24 maggio 2019, n. 36121; Cass. pen., sez. II, sentenza 14 luglio 2016, n. 33074; Cass. pen., sez. II, sentenza 14 luglio 2016, n. 33076.
[204] Cass. pen., sez. II, sentenza 7 luglio 2022, n. 27024 e Cass. pen., sez. II, 7 luglio 2022, n. 27023. Sempre in merito all'acquisto di criptovalute v. anche Cass. pen., sez. II, sentenza 7 ottobre 2021, n. 2868.
[205] Cass. pen., sez. II, sentenza 24 maggio 2019, n. 36121.
[206] DELL'OSSO A.M., *Sub art. 648-ter.1*, cit., p. 2333.
[207] ACQUAROLI R., *L'autoriciclaggio*, in C. Piergallini, F. Viganò, M. Vizzardi, A. Verri (a cura di), *I delitti contro la persona. Libertà personale, sessuale e morale, domicilio e segreti*, in *Trattato di diritto penale. Parte speciale*, diretto da G. Marinucci ed E. Dolcini, Padova, 2015, Vol. X, p. 943 ss., p. 949.

beni di provenienza illecita da parte dell'autore o del concorrente nel reato presupposto. Tuttavia, il fatto che la norma sanzioni chi impiega il danaro, i beni o le altre utilità provenienti da reato, mentre esenti da responsabilità penale i casi di mera utilizzazione e godimento personale del bene, è stato oggetto di critiche. In particolare, si evidenzia che non appare corretto ritenere che l'impiego dei proventi del reato per l'avvio di un'attività produttiva meriti discredito, riprovazione e conseguente punizione, mentre il godimento individuale degli stessi costituisca attività lodevole e, pertanto, andare esente da sanzione penale[208].

Difficoltosa è la precisa individuazione della funzione di disciplina della clausola, nonché quali siano i casi di "mera utilizzazione" o "godimento personale". Per una parte della dottrina tale clausola ha funzione di delimitazione dell'ambito di applicabilità della fattispecie e segna un limite negativo del tipo, perché descrive una modalità della condotta espressamente esclusa dalla rilevanza penale[209]. Essa, dunque, distingue le condotte di mero godimento e utilizzazione da quelle di cui al primo co. dell'art. 648-*ter*.1 c.p., dotate di carattere necessariamente dissimulatorio[210]. Si evidenzia, però, che in questo caso la clausola si limiterebbe a ribadire che le condotte atipiche sono irrilevanti[211]. Per altri autori, invece, clausola ha una mera valenza prescrittiva, fungendo da monito per la giurisprudenza a non punire come autoriciclaggio il mero consumo di utilità lecite[212]. Si evidenzia, però, che i concetti di utilizzazione e godimento personale appaiono comunque eccessivamente vaghi[213]. Sul punto, la giurisprudenza ritiene che la clausola di non punibilità prevista al comma in questione vada interpretata in senso letterale, per cui l'esclusione della responsabilità penale opera solo e soltanto se il soggetto utilizzi o goda dei beni provento del delitto presupposto in modo diretto e senza il compimento di alcuna operazione atta ad ostacolare concretamente l'identificazione della loro provenienza delittuosa[214].

Infine, anche tale reato contempla una circostanza aggravante speciale per i fatti commessi nell'esercizio di un'attività bancaria o finanziaria o di altra attività professionale. Sono poi previste due circostanze attenuanti speciali, a seguito della modifica di cui al d.lgs. 195/2021 entrambe ad effetto comune[215]. La prima trova applicazione qualora il reato

[208] SGUBBI F., *Il nuovo delitto di "autoriciclaggio"*, cit., p. 138.
[209] PIERGALLINI C., *Autoriciclaggio, concorso di persone e responsabilità dell'ente*, cit., p. 545.
[210] BASILE E., *L'autoriciclaggio nel sistema penalistico di contrasto*, cit., p. 1289.
[211] DELL'OSSO A.M., *Riciclaggio Di Proventi Illeciti*, cit., p. 208.
[212] SEMINARA S., *Spunti interpretativi sul delitto di autoriciclaggio*, cit., p. 1641.
[213] DELL'OSSO A.M., *Sub art. 648-ter.1*, cit., p. 2333.
[214] Cass. pen., sez. VI, sentenza 4 maggio 2020, n. 13571; Cass. pen., sez. II, sentenza 11 marzo 2020, n. 9755; Cass. pen., sez. II, sentenza 29 marzo 2019, n. 13795; Cass. pen., sez. II, sentenza 5 luglio 2018, n. 30399.
[215] PESTELLI G., *Riflessioni critiche sulla riforma dei reati di ricettazione*, cit., p. 51.

presupposto sia un delitto per il quale è stabilita la pena della reclusione inferiore nel massimo a cinque anni. La seconda, invece, è prevista per colui che si sia efficacemente adoperato per evitare che le condotte siano portate a conseguenze ulteriori o per assicurare le prove del reato e l'individuazione dei beni, del denaro e delle altre utilità provenienti dal delitto.

3.4. Le fattispecie di cui all'art. 55 d.lgs. 231/2007

Tutte le fattispecie esaminate nei paragrafi precedenti sono accomunate dal fatto che l'intervento penale è destinato alla repressione di comportamenti già attuati. Esse, infatti, operano quando il riciclaggio o il reinvestimento si sono già verificati[216]. L'Unione Europea, però, ritenne sin da subito che il controllo e la prevenzione delle infiltrazioni di denaro sporco non possono essere affidati solo agli strumenti di repressione *a posteriori* da parte della giustizia penale, ma è necessario regolamentare a monte l'attività d'intermediazione creditizia e mobiliare. Pertanto, attraverso le direttive antiriciclaggio sopra esaminate (v. *supra*, par. 2), ha previsto una serie di obblighi per gli intermediari bancari e finanziari, i quali sono dunque tenuti ad offrire la loro collaborazione.

Alcuni degli obblighi previsti dalla normativa antiriciclaggio sono oggi penalmente sanzionati dall'art. 55 del d.lgs. 231/2007. Qui, dunque, la norma penale non riguarda fatti di riciclaggio, ma il rafforzamento di obblighi di rilevazione, documentazione e comunicazione, in modo da dissuadere il successivo compimento di atti di riciclaggio[217]. L'obiettivo generale delle fattispecie in esame, infatti, è la protezione dell'integrità del sistema bancario e finanziario e, indirettamente, la protezione della sua stabilità[218].

Con il d.l. 3 maggio 1991, n. 143, convertito con modificazioni dalla legge antiriciclaggio 5 luglio 1991, n. 197, furono introdotte per la prima volta delle disposizioni penali volte a sanzionare gli obblighi previsti dalla normativa antiriciclaggio. In tale occasione vennero criminalizzate condotte meramente strumentali, quali la mancata rilevazione o archiviazione dei dati e bagatellizzate condotte essenziali nella lotta al riciclaggio, quali la violazione dell'obbligo di segnalazione da parte dei soggetti obbligati di operazioni sospette, sanzionate solo in via amministrativa[219]. Alcuni autori ritenevano, infatti, che l'obbligo di segnalazione delle operazioni "sospette", proprio per il ruolo cruciale

[216] *Ibid*., p. 1223.
[217] PECORELLA G., *Circolazione del denaro e riciclaggio*, cit., p. 1224.
[218] Cass. pen., sez. II, sentenza 20 febbraio 2015, n. 18141.
[219] MOCCIA S., *Effettività e normativa antiriciclaggio*, cit., p. 305.

nella prevenzione del riciclaggio, meritasse di essere sanzionato penalmente in una disposizione *ad hoc*, magari inserita nel codice penale[220].

Le fattispecie in materia di violazione degli obblighi della normativa antiriciclaggio sono poi state modificate ed inserite nell'art. 55 del d.lgs. 231/2007. Le fattispecie che prevedevano la sola pena della multa, ovvero quelle di cui all'originario co. 1 (violazione degli obblighi di identificazione) 4 (omessa o tardiva registrazione) e 7 (omissione delle comunicazioni previste) sono poi state depenalizzate dall'art. 1, c. 1 del d.lgs. 15 gennaio 2016, n. 8. La norma, infine, è stata modificata dal d.lgs. 25 maggio 2017, n. 90. Oggi, dunque, la norma di cui all'art. 55 prevede cinque reati distinti. Inizialmente tutti i reati previsti dall'originario art. 55 erano costruiti sullo schema dei reati d'obbligo[221]. Oggi, però, a seguito delle modifiche legislative, non è più così, dato che a sanzionare la mera violazione di un obbligo è unicamente il co. 4, mentre gli altri reati sanzionano la falsificazione e l'utilizzazione, l'acquisizione o conservazione di dati falsi.

Al primo comma sono previsti due delitti. Il primo sanziona colui che, essendo tenuto all'osservanza degli obblighi di adeguata verifica ai sensi del d.lgs. 231/2007, falsifica i dati e le informazioni relative al cliente, al titolare effettivo, all'esecutore, allo scopo e alla natura del rapporto continuativo o della prestazione professionale e all'operazione. Il secondo, invece, punisce con pena identica il medesimo soggetto, qualora, in occasione dell'adempimento degli obblighi di verifica, utilizzi dati e informazioni falsi relativi al cliente, al titolare effettivo, all'esecutore, allo scopo e alla natura del rapporto continuativo o della prestazione professionale e all'operazione.

Il secondo comma prevede un delitto a carico di colui che, essendo tenuto all'osservanza degli obblighi di conservazione ai sensi del d.lgs. 231/2007, acquisisce o conserva dati falsi o informazioni non veritiere sul cliente, sul titolare effettivo, sull'esecutore, sullo scopo e sulla natura del rapporto continuativo o della prestazione professionale e sull'operazione, ovvero si avvale di mezzi fraudolenti al fine di pregiudicare la corretta conservazione dei predetti dati e informazioni. Il terzo comma, invece, sanziona l'obbligato a fornire i dati e le informazioni necessarie ai fini dell'adeguata verifica della clientela, che fornisce dati falsi o informazioni non veritiere. In quest'ultimo caso è prevista una clausola di sussidiarietà espressa. Tutte e quattro le fattispecie esaminate sono punite con la reclusione da sei mesi a tre anni e con la multa da 10.000 euro a 30.000 euro. Non si tratta più, pertanto, di reati bagatellari.

[220] MOCCIA S., *Impiego di capitali illeciti e riciclaggio*, cit., p. 747.
[221] *Ibid*.

Al quarto comma, invece, vi è una contravvenzione a carico di chiunque, essendovi tenuto, violi il divieto di comunicazione di cui agli artt. 39, co. 1, che consiste nel divieto di avvisare il cliente o il terzo del fatto che l'operazione sospetta da loro compiuta è stata segnalata e 41, co. 3 d.lgs. 231/2007, nonché sul flusso di ritorno delle informazioni. Quest'ultima norma, però, è stata abrogata dal d.lgs. 90/2017, per cui, in mancanza del relativo obbligo, tale condotta non può essere sanzionata penalmente. Anche in questo caso è prevista una clausola di sussidiarietà espressa, per cui va escluso il concorso con altri reati puniti più severamente.

Come si può notare, si tratta in tutti i casi di reati propri, che possono essere commessi unicamente dai soggetti obbligati ai sensi della normativa antiriciclaggio. A seguito dell'inserimento degli *exchanger* e dei *wallet provider* tra i soggetti sottoposti agli obblighi in materia di antiriciclaggio, si deve necessariamente concludere che anch'essi possono essere soggetti attivi delle fattispecie contemplate dall'art. 55 del d.lgs. 231/2007[222]. Va però evidenziato che raramente gli *exchanger* e i *wallet* provider falsificano i dati e le informazioni relative al cliente o comunque fanno utilizzo di dati falsi ad esso relativi. Casomai, quello sì, non effettueranno alcuna verifica sulla sua identità, condotta che, però, non è penalmente sanzionata dalle norme in questione. Non sembra, dunque, che l'estensione delle fattispecie in esame a tali soggetti possa costituire un valido elemento per contrastare il fenomeno del *cyberlaundering* commesso tramite criptovalute. Ulteriore problema non di poco momento è poi la realizzabilità pratica di tale disposizione. Va, infatti, ribadito che gli *exchanger* e *wallet provider*, a differenza di banche ed intermediari finanziari, non operano su mercati regolamentati e spesso gli scambi avvengono nel totale anonimato nel *darkweb*. Pertanto, anche l'estensione delle fattispecie in materia di antiriciclaggio di cui all'art. 55 d.lgs. 231/2007 ai prestatori di valute virtuali sembra costituire un altro esempio di diritto penale meramente simbolico.

4. Il ruolo dei c.d. *financial managers*

Nell'ambito del riciclaggio, una tecnica particolarmente efficace per nascondere la provenienza delittuosa del denaro consiste nell'impiego dei c.d. *financial managers*. Con l'appellativo di *financial manager*, detto anche agente finanziario o prestaconto, si identifica colui che mette a disposizione un conto corrente per una certa persona, sul quale viene versata una data somma, dalla vittima della frode oppure dall'autore del reato, che egli ha il

[222] VADALÁ R.M., *Criptovalute e cyberlaundering*, cit.

compito di ritrasferire su un altro conto corrente, spesso di un Paese diverso, in cambio di un corrispettivo o di una percentuale sulla somma versata sul suo conto. Facendosi versare tale somma di denaro, il soggetto entra in possesso di fondi di illecita provenienza, di cui poi, attraverso l'ulteriore trasferimento da lui attuato, occulta l'origine.

Il c.d. *financial manager* classico mette a disposizione i propri conti correnti per ricevere una data somma di denaro e poi trasferirla su un altro conto corrente bancario, dopo aver detratto la quota concordata[223]. Vi sono poi gli agenti finanziari c.d. di vendita[224]. Questi ultimi, sempre in cambio di un corrispettivo, si occupano di ricevere la merce illecitamente acquistata da terze persone tramite *carding* su siti *Internet* quali Amazon, e-bay e simili. Dopodiché si occupano di rispedire a loro volta la merce ad un determinato indirizzo che viene ad essi fornito, in modo da renderne più difficile l'individuazione, oppure di consegnarla ad altre persone. In altri casi, agli agenti finanziari viene richiesto di prelevare in contanti da apposite carte di pagamento ricaricabili, sulle quali è contenuto il denaro versato dalle vittime delle frodi informatiche, contanti che poi devono a loro volta trasferire all'estero via *Western Union* e/o *Money Gram*. In altri casi ancora i *financial manager* vengono impiegati per mascherare l'origine illegale delle criptovalute. Esistono, infatti, fornitori di appositi servizi che offuscano le transazioni sulla *blockchain*. In particolare, essi si occupano di scambiare le criptovalute di diversi utenti suddividendoli tra diversi indirizzi di destinazione ad intervalli casuali, in modo che dalla *blockchain* risulti che nello stesso momento vi sono state più transazioni per importi congruenti. In questo modo diviene difficile ricostruire l'originaria catena di blocchi ed individuare la destinazione finale delle criptovalute che costituiscono provento di reato[225].

I *financial manager* non sono tutti uguali. Come già accennato (v. *infra*, cap. I, par. 4), alcuni di essi hanno conoscenze specialistiche del mondo della finanza e prestano volontariamente i propri servizi illeciti a titolo professionale. Spesso si tratta di società fantasma o di membri di associazioni a delinquere, che si dedicano al trasferimento di fondi da un conto all'altro dietro compenso o che si occupano di aprire e gestire conti correnti *offshore*, ad esempio a Panama, nelle Isole Cayman o nel Belize[226]. In questo caso, l'agente finanziario ha sufficiente contezza della commissione del reato presupposto di frode informatica e quindi agisce dolosamente. Ma spesso i *financial manager* non sono che privati

[223] KOCHHEIM D., *Cybercrime und Strafrecht in oder Informations- und Kommunikationstechnik*, München, 2018, p. 157 ss.
[224] QUEDENFELD R., *Handbuch Bekämpfung der Geldwäsche*, zit., s. 244.
[225] MAUME P., MAUTE L., *Rechtshandbuch Kryptowerte*, cit., s. 29.
[226] PLANTAMURA V., *Il cybericiclaggio*, cit., p. 872.

cittadini, che vengono reclutati via *mail* dai criminali informatici. Di solito, questi agenti finanziari, spesso socialmente svantaggiati o anziani, non hanno un'idea sufficiente del fatto che il denaro o i beni che trasferiscono sono provento di reato e quindi non agiscono dolosamente. In molti casi sono stati essi stessi ingannati con false offerte di lavoro. Vi è, però, chi evidenzia che ormai la gran parte dei *financial manager* non sono quasi più vittime innocenti del *phisher*, bensì si tratta di persone in cerca di facili guadagni, non particolarmente preoccupate per le conseguenze legali delle loro azioni e che ormai quella del *financial manager* viene considerata una vera e propria professione. Spesso si tratta di società fantasma che si fingono "consulenti finanziari", mentre in realtà offrono ai *phisher* diversi servizi per nascondere la provenienza delittuosa del denaro, occupandosi direttamente di reclutare i *financial manager*[227]. Spesso, poi, per una singola operazione vengono impiegati molti agenti finanziari, perché più le somme di denaro, le criptovalute o i beni provento di reato vengono scambiati, più diventa difficile risalire alla loro origine.

L'individuazione del titolo di reato cui tali soggetti sino chiamati a rispondere penalmente non è certamente un'operazione facile. In molti casi la giurisprudenza ha ritenuto che la condotta di tali soggetti integri il reato di riciclaggio di cui agli artt. 648-*bis* c.p. È stato infatti osservato che se il *financial manager* si limita a ricevere il denaro illecito sul suo conto corrente ed a ritrasferirlo su un altro, non può essere considerato concorrente nel reato presupposto, in particolare la frode informatica, dato che quest'ultimo reato si è già consumato[228]. Si pone, però, un grosso problema con riferimento alla sussistenza dell'elemento soggettivo del reato di riciclaggio. *Nulla quaestio* con riferimento a quelle persone che offrono volontariamente i loro servizi al *phisher*, perché esse sono a conoscenza del fatto che le somme o i beni che debbono trasferire costituiscono provento di un reato cibernetico. Peraltro, in quest'ultimo caso, qualora il reo si offra volontariamente di offrire tale servizio dietro corrispettivo agendo in maniera continuativa, può pure configurarsi la circostanza aggravante del fatto commesso nell'esercizio di un'attività professionale, dato che per la configurabilità della circostanza in questione non è richiesto che il soggetto sia iscritto in un apposito albo o che l'attività richieda una speciale abilitazione. Tuttavia, come evidenziato, in molti casi l'agente finanziario non è che un soggetto convinto di agire lecitamente in base ad un valido contratto di lavoro e non è a conoscenza del fatto che il

[227] LORENZANA GONZÁLEZ C., *Fraude y estafas electrónicas*, in C. Sanchis Crespo (a cura di), *Fraude electrónico. Panorámica actual y medios jurídicos para combatirlo*, Cizur menor, 2013, p. 25 ss., p. 37.
[228] Cass. pen., sez. II, sentenza 9 febbraio 2017, n. 10060; per la dottrina v. PIANCASTELLI S., *La ricezione di somme di denaro provento di phishing: risultanze investigative e problemi applicativi in punto di qualificazione giuridica*, in *Dir. pen. cont*., 2015, p. 1 ss., p. 5.

denaro o i beni che deve trasferire ad altri sono in realtà provento di reato. A tal proposito, va ribadito che nel nostro codice penale non è prevista la punibilità del riciclaggio a titolo di colpa. Tuttavia, si ritiene che l'elemento soggettivo del reato in questione possa essere costituito anche dal dolo eventuale. Per questo motivo, la giurisprudenza, sia della Corte di Cassazione che di merito, in alcune occasioni ha condannato il *financial manager* per riciclaggio a titolo di dolo eventuale[229]. In particolare, è stato evidenziato come sia ormai noto al grande pubblico che lo svolgimento di attività del genere sia di carattere illecito, dunque il soggetto ben può rappresentarsi il fatto che il denaro o i beni a lui trasferiti costituiscono provento di reato. Il fatto che gli venga affidata una grossa somma di denaro da parte di uno sconosciuto senza apparente motivo dietro un corrispettivo sproporzionato se rapportato alla semplicità dell'attività da svolgere, sono tutti indici di sospetto che dovrebbero indurre qualsiasi utente in buona fede a dubitare della legalità dell'attività che gli si chiede di svolgere. Pertanto, la giurisprudenza ritiene sussistente il dolo nella sua forma eventuale, dato che l'agente ha la concreta possibilità di rappresentarsi il fatto che il denaro ricevuto ed investito sia di provenienza delittuosa e decide di agire comunque, accettandone il rischio.

Questa interpretazione ha suscitato delle critiche in dottrina, perché porta ad una rilevante estensione della responsabilità penale[230]. Infatti, in molti casi l'elemento soggettivo del reato finisce così per essere inaccettabilmente presunto, per non essersi l'agente adeguatamente informato in merito alla natura dell'attività da lui svolta. Peraltro, tale interpretazione, che pone l'accento sul sospetto del *financial manager*, stride con l'interpretazione fornita dalle stesse Sezioni Unite della Corte di Cassazione in merito alla configurabilità del dolo eventuale nel delitto di ricettazione, le quali hanno sottolineato che il dolo eventuale non può essere desunto da semplici motivi di sospetto e non può consistere in un mero sospetto[231]. Inoltre, il dolo eventuale, come ribadito dalle Sezioni Unite[232], esige che si sappia o si possa concludere che il soggetto era comunque orientato ad agire e, pertanto, lo avrebbe fatto pure nel caso in cui avesse avuto la certezza della provenienza illecita della cosa. In questo caso, però, la responsabilità del *financial manager* a titolo di

[229] Cass. pen., sez. II, sentenza 8 giugno 2021, n. 22475; Corte appello Ancona, sentenza 23 febbraio 2021, n.1607; Tribunale di Milano, sentenza 7 ottobre 2011, in *Dir. pen. proc.*, 2012, n. 1, s. 55.
[230] FLOR R., *Phishing e profili penali dell'attività illecita di "intermediazione" del c.d. financial manager*, in *Dir. pen. proc.*, 2012, s. 55 ff., s. 65.
[231] Cass. pen., sez. un., sentenza 26 novembre 2009, n. 12433, con nota di DONINI M., *Dolo eventuale e formula di Frank nella ricettazione. Le Sezioni Unite riscoprono l'elemento psicologico*, in *Cass. Pen.*, 2010, n. 7-8, p. 2555 ss.
[232] Cass. pen., sez. un., sentenza 24 aprile 2014, n. 38343.

riciclaggio viene affermata sulla base del fatto che egli poteva dubitare della liceità dell'attività lui richiesta. In passato, la Corte di Cassazione si è mostrata più rigorosa in merito all'accertamento del dolo, tant'è che escludeva la responsabilità penale per riciclaggio dell'agente finanziario che avesse solo un mero sospetto sull'origine dei beni, ritenendo necessaria la consapevolezza concreta della provenienza della cosa da delitto[233].

Va però evidenziato che la giurisprudenza non è unanime nel ritenere che l'agente finanziario che ritira i fondi che gli sono stati trasferiti sul suo conto direttamente dalla vittima e li trasferisca al *phisher* dopo aver dedotto la sua commissione, risponda necessariamente a titolo di riciclaggio. Una parte della giurisprudenza, infatti, ritiene che in questo caso il prestaconto debba rispondere a titolo di concorso in frode informatica[234]. In particolare, si evidenzia che la frode informatica si consuma nel momento in cui il soggetto agente consegue l'ingiusto profitto con correlativo danno patrimoniale, per cui la condotta di colui che mette a disposizione di terzi il proprio conto corrente per ricevere direttamente la somma di denaro conseguita mediante accesso abusivo al sistema informatico altrui si inserisce direttamente nella fase di esecuzione di tale reato. Infatti, il contributo del *financial manager* agevola e rende possibile il conseguimento del profitto della frode informatica[235]. A tal proposito, si è ritenuto che il fatto che non sia stato individuato il soggetto che materialmente abbia commesso la frode informatica manipolando il sistema ed eseguendo il trasferimento non autorizzato del denaro della vittima non vale ad escludere il concorso ex art. 110 c.p. nel reato frode informatica del *financial manager* titolare del conto corrente o della carta di credito su cui sono state illegittimamente riversate le somme prelevate dal conto della persona offesa[236].

Questa soluzione non è unanimemente condivisa. Infatti, la stessa giurisprudenza della Suprema Corte non è univoca nello stabilire quando si verifica esattamente la consumazione del reato di frode informatica. In alcuni casi, ha sostenuto che il reato si consumi nel momento in cui il reo interviene sui dati del sistema informatico, alterandone il funzionamento[237]. Tuttavia in altre sentenze ha ritenuto il contrario, affermando che la frode informatica si consuma solo quando le somme vengono accreditate sul conto corrente[238].

---

[233] Cass. pen., sez. II, sentenza 1 luglio 2011, n. 25960.
[234] Cass. pen., sez. II, sentenza 12 settembre 2018, n. 5748; Trib. Milano, sez. VI penale, sentenza 28 maggio 2013, n. 6753 in dirittopenaleuomo.org.
[235] Cass. pen., sez. II, sentenza 27 maggio 2020, n. 16023; Cass. pen., sez. II, sentenza 10 settembre 2018, n. 48553.
[236] Cass. pen., sez. II, sentenza 12 settembre 2018, n. 5748.
[237] Cass. pen., sez. V, sentenza 19 febbraio 2015, n. 32383; Cass. pen., sez. II, sentenza 25 gennaio 2011, n. 6958.
[238] Cass. pen., sez. II, sentenza 9 febbraio 2017, n. 10060.

Seguendo tale ultima soluzione, dunque, il *financial manager* risponde a titolo di concorso nella frode informatica nel caso in cui sia consapevole dell'attività truffaldina del *phisher* ed assicuri a questi la propria collaborazione nel ricevere bonifici fraudolenti e quindi nel trasferire a terze persone ignote le somme percepite. Al contrario, risponde per il reato di riciclaggio a titolo di dolo eventuale nel caso in cui riceva solo la mera richiesta di farsi accreditare somme su un proprio conto corrente e di trasferire successivamente in altro modo le somme di denaro così ricevute all'estero e, quindi, sia inconsapevole del disegno criminoso complessivo, per cui non sussistono i presupposti per la sussistenza del concorso doloso nel reato presupposto[239].

Pertanto, le stesse persone, che compiono la medesima azione, rispondono a titolo di concorso nel reato presupposto o di riciclaggio a seconda che abbiano o meno il dolo di favoreggiamento. Tuttavia, va evidenziato che il riciclaggio è punito molto più gravemente rispetto alla frode informatica. Per cui, seguendo tale tesi si arriva al paradosso di punire più gravemente il prestaconto che non ha la piena conoscenza che il denaro da lui ricevuto costituisce provento di reato rispetto a quello che agisce dolosamente quale complice del reato cibernetico al fine di prestare ausilio al *phisher*.

Va poi evidenziato che spesso per compiere un'unica operazione vengono impiegati moltissimi *financial manager*, in modo da rendere ancora più difficile l'individuazione dell'origine delittuosa del denaro. Vengono così effettuati svariati trasferimenti di denaro tra i loro diversi conti correnti prima di arrivare alla destinazione definitiva, che è il conto corrente dell'autore dell'illecito. Nel caso in cui il primo *financial manager* che ha ricevuto il denaro direttamente dalla vittima lo trasferisca ad un altro *financial manager*, quest'ultimo sicuramente non può essere sanzionato a titolo di frode informatica, poiché quest'ultima si è già consumata prima di tale trasferimento. Pertanto, seguendo la teoria di cui sopra, due soggetti che compiono sostanzialmente la medesima azione ed hanno entrambi la consapevolezza che il denaro costituisce provento di reato, vengono puniti a diverso titolo unicamente in base alla loro collocazione temporale nella "catena" di riciclaggio. Questa soluzione, dunque, non è assolutamente soddisfacente e viola il principio di uguaglianza. Tuttavia, non appare corretta neppure la prima soluzione proposta, ovvero ritenere che tutti i *financial manager* rispondano a titolo di riciclaggio anche a titolo di dolo eventuale, qualora accettino il rischio che le somme di denaro o i beni da loro ricevuti costituiscono provento di reato. In questo modo, infatti, tali soggetti finiscono per essere sanzionati con pena molto

[239] Tribunale di Vicenza, sez. penale, sentenza 3 marzo 2022, n. 120, in *Dejure*.

più grave rispetto a quella dell'autore del reato presupposto, anche senza avere piena contezza del disvalore complessivo del fatto. Si ritiene, dunque, opportuna una modifica legislativa che prenda in considerazione la peculiare posizione dei *financial manager*, in particolar modo con riferimento all'elemento soggettivo. A tal fine, nel prossimo capitolo si esaminerà se, a che titolo e con quale pena tali soggetti vengono sanzionati negli ordinamenti tedesco e spagnolo, in modo da verificare se le soluzioni ivi adottate possono essere soddisfacenti ed offrire spunti per una riforma della normativa in questione.

Va poi evidenziato che a seguito dell'introduzione del reato di autoriciclaggio, l'autore del *phishing*, qualora dia un incarico a un prestanome di trasferire il denaro o egli stesso lo impieghi in attività economiche, finanziarie, imprenditoriali o speculative, sarà punibile non solo per il reato presupposto ma anche per tale ultimo reato. Tuttavia, come evidenziato in precedenza, l'autoriciclaggio è un reato proprio e prevede una pena più mite rispetto al riciclaggio di denaro. Pertanto, in ogni caso il *financial manager* viene punito più severamente del *phisher*. In questi casi, tuttavia, è prevista una pena più lieve perché il reato presupposto di frode informatica prevede la pena della reclusione non superiore a cinque anni.

Infine, non va dimenticato che i *financial manager* reclutati *online* che agiscono professionalmente offrendosi di occultare la provenienza delittuosa di una singola transazione, spesso sono componenti di associazioni a delinquere. Si pone, dunque, il problema dell'individuazione del titolo di reato per cui essi sono chiamati a rispondere, dato che il denaro riciclato è frutto delle attività illecite dell'organizzazione criminale dedita agli attacchi informatici. Si evidenzia che nelle nuove strutture organizzate che operano sul *web* diverse dalle associazioni a delinquere di stampo tradizionale, non vi è una suddivisione gerarchica, ma per specifici compiti. Dunque, i *financial manager* spesso partecipano all'associazione solo col particolare ruolo di "riciclatore", senza prendere parte ai delitti programmati, per cui possono rispondere sia del reato di associazione a delinquere che di riciclaggio[240].

[240] ZANCHETTI M., *Il riciclaggio di denaro*, cit., p. 356, che evidenzia che l'oggetto del riciclaggio dev'essere limitato all'"arricchimento criminale", a beni che entrano nel patrimonio del reo attraverso il delitto, mentre la mera partecipazione ad un'associazione criminale è a ciò inidonea. *Contra* TURONE G., *Il delitto di associazione mafiosa*, Milano, 1995, p. 373 ss.

5. Considerazioni di sintesi

Dall'analisi effettuata emerge come il sistema repressivo del fenomeno del riciclaggio nel suo complesso, dunque comprensivo anche del *cyberlaundering*, sia estremamente capillare ed articolato. Il numero di fattispecie in vigore, tra quelle di tipo preventivo e repressivo, è particolarmente elevato. Anche in questo caso si concorda con coloro che evidenziano che le fattispecie in vigore sono già sufficientemente ampie, al punto da essere addirittura sovrabbondanti[241]. Infatti, anche se il fenomeno del *cyberlaundering* non è espressamente regolato, esso rientra già nell'ambito applicativo delle norme vigenti. Dunque, l'introduzione di un nuovo reato non solo sarebbe assolutamente superflua, ma rischierebbe di dar luogo agli stessi problemi relativi all'individuazione dei rapporti tra le diverse fattispecie di cui si è dato conto nei capitoli precedenti con riferimento ai reati cibernetici. Tuttavia, le fattispecie contemplate dall'art. 55 del d.lgs. 231/2007 non si rilevano pienamente idonee a punire le condotte prodromiche alla commissione del riciclaggio tramite le criptovalute, dato che difficilmente esso viene commesso tramite la falsificazione dei dati relativi alle monete virtuali. In tale ottica, sarebbe forse più opportuno sanzionare penalmente l'omissione dell'obbligo di identificazione degli acquirenti delle criptovalute.

È poi da accogliere con favore la scelta del legislatore italiano di non sanzionare il mero possesso o l'utilizzazione dei proventi illeciti. Sul punto, si concorda con coloro che ritengono sia impossibile pretendere *a priori* di contrastare un processo economico complesso e multiforme come il riciclaggio. Una fattispecie che lo sanzioni è indispensabile, ma la stessa deve porsi lo scopo limitato di contrastare alcuni comportamenti particolarmente insidiosi o particolarmente adatti ad essere contrastati col mezzo della norma penale[242], cosa che invece, le condotte di possesso e utilizzazione non sono.

Per quanto riguarda poi specificamente il fenomeno del *cyberlaundering*, sebbene vi sia sostanziale concordia in merito all'inutilità dell'introduzione di una fattispecie penale *ad hoc*, qualche autore ha ipotizzato la necessità di prevedere una circostanza aggravante speciale, valida per tutte e tre le fattispecie incriminatrici previste dal codice penale. Questo perché si ritiene che le condotte di riciclaggio poste in essere tramite strumenti informatici si caratterizzino per una maggiore gravità[243]. Tuttavia, posto che il *cyberlaundering* si sta diffondendo sempre di più e che probabilmente il riciclaggio commesso mediante lo

[241] PICOTTI L., *Profili penali del cyberlaundering*, cit., p. 614.
[242] ZANCHETTI M., *Il riciclaggio di denaro*, cit., p. 169.
[243] PLANTAMURA V., *Il cybericiclaggio*, cit., p. 888.

spostamento fisico di valigie di contanti finirà per diventare marginale, vi è il rischio che accada esattamente quel che è successo per la frode informatica con l'introduzione dell'ultima circostanza aggravante del trasferimento del valore monetario e della valuta virtuale, ovvero che l'ipotesi aggravata finisca per diventare "di fatto" l'ipotesi ordinaria di reato. Non si vede, quindi, la necessità di introdurre una circostanza aggravante del genere, anche tenendo conto del fatto che le pene previste per i reati di riciclaggio sono già particolarmente elevate.

Infine, per quanto riguarda specificamente i *financial manager*, si ritiene che le soluzioni sinora individuate in merito alla loro responsabilità penale non siano affatto soddisfacenti, per cui tale aspetto appare assolutamente meritevole di un ripensamento da parte del legislatore. Nel prossimo capitolo si effettuerà un'analisi della normativa tedesca e spagnola in materia di reati cibernetici contro il patrimonio, comprese le norme volte a sanzionare il *cyberlaundering*, al fine di verificare se le soluzioni ivi presenti possano fungere da modello ed esempio per il nostro ordinamento, anche con riguardo alla punibilità dei *financial manager*.

Capitolo V

La tutela penale del patrimonio dalle minacce cibernetiche nell'esperienza giuridica tedesca e spagnola

Sommario: 1. Ambito, scopi ed utilità dell'indagine comparata sui reati cibernetici. – 1.1. Il contrasto alla criminalità patrimoniale e informatica in Germania: inquadramento generale. – 1.2. Segue: in Spagna. – 2. La rilevanza penale degli atti preparatori alla commissione di più gravi reati *lato sensu* patrimoniali; - 2.1. Le norme in materia di contraffazione; - 2.2. Gli atti preparatori alla falsificazione e indebito utilizzo di strumenti di pagamento diverso dai contanti; - 2.3. Gli atti preparatori alla commissione della frode informatica. – 3. La fase di interazione con i dati illecitamente carpiti; - 3.1. L'accesso abusivo al sistema informatico; - 3.2. L'intercettazione di dati; 3.3. La ricettazione di dati; 3.4. Le fattispecie a tutela dei dati personali. – 4. L'ottenimento dell'ingiusto profitto: truffa, estorsione e frode informatica; - 4.1. La truffa; - 4.2. L'estorsione; - 4.3. La frode informatica. – 5. La falsificazione e l'indebito uso degli strumenti di pagamento diversi dal contante. – 6. I reati contro la disponibilità, l'integrità e la funzionalità dei dati e dei sistemi informatici; - 6.1. L'interferenza nei confronti dei dati; - 6.2. L'interferenza nei confronti dei sistemi informatici. – 7. La responsabilità penale dei gestori di piattaforme illegali di scambio: il nuovo § 127 StGB. - 7.1. Segue: sull'opportunità di introdurre una fattispecie incriminatrice di ugual tenore nell'ordinamento italiano. – 8. La disciplina penale del riciclaggio; - 8.1. Le condotte sanzionate, - 8.2. L'oggetto del reato; - 8.3. L'elemento soggettivo; - 8.4. La punibilità dell'autoriciclaggio. – 9. La responsabilità penale dei *financial manager*. – 10. Riflessioni conclusive.

1. Ambito, scopi ed utilità dell'indagine comparata sui reati cibernetici

La dimensione transnazionale del *cybercrime* pone nuove sfide sia per il legislatore nazionale che per le autorità di *law enforcement,* perché la singola iniziativa presa a livello statale rischia di rivelarsi inefficace. Infatti, il diritto penale nazionale è normalmente se si dispone limitato al territorio nazionale, ove le pronunce giudiziarie hanno valore unicamente in quel territorio, per cui diventa difficile contrastare questi fenomeni che, invece presentano un'evidente dimensione internazionale. Pertanto, il legislatore europeo ha avvertito molto

presto la necessità di un'azione congiunta tra gli Stati membri per la repressione di questo nuovo fenomeno criminoso chiamato *cybercrime*.

A seguito dell'entrata in vigore del Trattato di Lisbona, la "criminalità informatica" è stata inserita nell'art. 83 par. 1 TFUE fra i fenomeni criminosi di natura grave e transnazionale su cui l'Unione Europea ha competenza penale, seppur indiretta, potendo stabilire norme minime relative alla definizione dei reati e delle sanzioni. (v. *supra*, cap. I par. 9). Non va però dimenticato che nell'ambito del diritto europeo, il diritto penale occupa una posizione peculiare rispetto alle altre branche del diritto. Infatti, per via della forte connessione con la sovranità dello Stato, è considerato un terreno sensibile, sul quale il legislatore europeo è ancora restio ad intervenire[1]. Tuttavia, vi sono fenomeni criminosi che non rappresentano peculiarità statali, tra cui la criminalità economica ed informatica, per cui in questi ambiti l'integrazione europea in campo penale può essere attuata senza il rischio di porsi in diretto contrasto con i valori etici e sociali che caratterizzano una data comunità[2]. Non a caso, tra i primi provvedimenti emanati dalla Comunità europea ancora prima dell'adozione del Trattato di Lisbona, vi sono proprio la Decisione quadro del Consiglio 2001/413/GAI relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti e la Decisione quadro del consiglio 2001/500/GAI concernente il riciclaggio di denaro.

La competenza penale del legislatore europeo con riferimento alla criminalità informatica, però, va ribadito, è solo indiretta. Questo significa che neppure in questo ambito il legislatore europeo può direttamente prevedere delle incriminazioni, ma può soltanto «*stabilire norme minime relative alla definizione dei reati e delle sanzioni*». Dunque, oltre alla definizione dei termini essenziali, il legislatore europeo può delineare una descrizione delle condotte che in ogni caso devono essere considerate reato. Inoltre, può prevedere requisiti di incriminazione che si riferiscono alla parte generale, ovvero l'obbligo di punire il tentativo, o il concorso di persone nel reato, o prevedere sanzioni a carico delle persone giuridiche[3]. Lo Stato membro, dunque, mantiene la facoltà (che peraltro anche in quest'ambito in passato è stata esercitata sia dal nostro legislatore che da quello degli altri Stati membri) di "andare oltre" questa regolamentazione minima stabilita nella direttiva, criminalizzando ulteriori comportamenti o stabilendo pene più severe. Nonostante i

[1] GREVE V., *Die Zukunft des Europäischen Strafrechts: Rechtsdogmatische Vorgaben*, in U. Sieber (a cura di), *Europäische Einigung und Europäisches Strafrecht*, Berlin, 1993, p. 107 ss., p. 109.
[2] SATZGER H., *International and European Criminal Law*, München, 2018, p. 76.
[3] *Ibid*., p. 90.

numerosi provvedimenti adottati in seno alle istituzioni europee, permangono significative differenze tra gli Stati membri nel diritto penale di contrasto alla criminalità informatica e cibernetica.

Ed ecco che la comparazione penale tra i diversi ordinamenti in ambito europeo in particolare assume una notevole importanza nel c.d. processo di europeizzazione del diritto penale, fondamentale per combattere fenomeni criminosi di natura transnazionale, perché richiede un costante coordinamento con gli ordinamenti giuridici dei singoli Stati nazionali se si vogliono evitare attriti e conflitti nella sua attuazione. Infatti, senza di essa è impossibile attuare iniziative penali a livello sovranazionale realmente idonee a raggiungere gli scopi perseguiti[4]. A tal proposito, va sottolineato che l'ulteriore creazione di diritto dell'Unione europea per raggiungere efficacemente gli obiettivi prefissati richiede un lavoro preliminare di comparazione del diritto vigente nei diversi Stati membri[5]. La comparazione, quindi, si rivela indispensabile per la creazione di nuovo diritto a livello europeo. Non solo, ma può essere utile anche per lo stesso legislatore nazionale quando decide autonomamente di riformare le norme vigenti o di sanzionare nuovi comportamenti criminosi, nonché quando deve dare attuazione a provvedimenti adottati a livello sovranazionale[6]. La comparazione tra i diversi ordinamenti, inoltre, permette di verificare il livello di ravvicinamento e armonizzazione raggiunta tra i diversi sistemi penali nazionali, in un ambito in cui, come si è osservato, il legislatore europeo è sempre più presente[7]. Tale verifica, infatti, permette di individuare nuovi ambiti in cui l'intervento del legislatore europeo può essere necessario. Peraltro, va evidenziato che anche in un settore come il diritto penale dell'informatica, oggetto di diversi interventi legislativi del legislatore europeo volto ad uniformare la materia nei diversi Stati membri, norme di diritto penale uguali o molto simili vengono applicate in maniera diversa a seconda, a causa dell'influenza della cultura giuridica propria del singolo Stato membro[8]. In quest'ambito, dunque, data la notevole somiglianza delle normative, che molto spesso presentano un'origine comune, è possibile svolgere un'analisi comparatistica

[4] SIEBER U., *Strafrechtsvergleichung im Wandel. Aufgaben, Methoden und Theorieansätze der vergleichenden Strafrechtswissenschaft*, in U. Sieber, H. Albrecht (a cura di), *Strafrecht und Kriminologie unter einem Dach. Kolloquium zum 90. Geburtstag von Professor Dr. Dr. h.c. mult. Hans-Heinrich Jeschek*, Berlin, 2006, p. 78 ss., p. 85.
[5] ESER A., *Comparative criminal law. Development. Aims, Methods*, München, 2017, p. 14.
[6] KREMNITZER M., *Some Reflections on Comparative Criminal Law*, in S. Beck, C. Buchard, B. Fateh-Moghadam (a cura di), *Strafrechtsvergleichung als Problem un Lösung*, Baden-Baden, 2011, p. 29 ss., p. 31.
[7] HILGENDORF E., *Zur Einführung: Globalisierung und Recht*, in S. Beck, C. Buchard, B. Fateh-Moghadam (a cura di), *Strafrechtsvergleichung als Problem un Lösung*, Baden-Baden, 2011, p. 11 ss., p. 24
[8] *Ibid*., p. 16.

anche ai fini dell'individuazione di soluzioni interpretative che possano adattarsi alla nostra legislazione senza per forza incorrere nel divieto di analogia *in malam partem*[9].

In questo capitolo si esaminerà dapprima la legislazione tedesca in materia di reati informatici e cibernetici contro il patrimonio, una delle più all'avanguardia nella lotta al *cybercrime* e che ha rappresentato e tutt'ora rappresenta un modello di riferimento per molti ordinamenti europei[10], tra cui quello italiano. Dopodiché si esaminerà la legislazione spagnola in tale ambito, trattandosi di uno dei Paesi europei che possiede una delle più recenti codificazioni penali in Europa (*Ley Orgánica 10/1995, de 23 de noviembre 1995*), che già nella sua formulazione originaria ha previsto l'incriminazione di alcune forme di criminalità informatica (v. ad es. Art. 248.2 *Código Penal - De las estafas*), nonché uno dei primi ad attuare la direttiva 2013/40/UE relativa agli attacchi contro i sistemi di informazione, con la *Ley Orgánica 1/2015, de 30 de marzo*. Pertanto, si procederà con un inquadramento generale in merito alla legislazione a tutela del patrimonio e in materia di criminalità informatica e cibernetica nei due Paesi, dopodiché si procederà all'analisi e al confronto tra le norme presenti nelle legislazioni dei due diversi paesi, con riferimento alle diverse fasi e tipologie di attacchi informatici contro il patrimonio. Rispetto all'analisi delle singole norme, ove possibile si privilegerà un approccio sistematico, diretto a mettere in evidenza le caratteristiche comuni e le differenze con la nostra legislazione penale in materia. Lo scopo di questo lavoro è proprio di esaminare quante e quali delle nuove manifestazioni criminose sopra descritte (v. *supra* cap. I) sono sanzionate dalla vigente legislazione tedesca e spagnola e, eventualmente, quali soluzioni interpretative sono state date alle norme vigenti e contemporaneamente identificare le fattispecie che ormai sono divenute obsolete e sono quindi di fatto disapplicate. Nell'analisi comparata, infatti, è importante distinguere tra *law in the books* e *law in action*[11]. A sua volta, tale analisi è finalizzata a stabilire se le soluzioni interpretative adottate in altri Paesi con legislazione simile alla nostra possono eventualmente essere utilizzate anche per risolvere i problemi applicativi già evidenziati nei capitoli precedenti. Inoltre, particolare attenzione sarà rivolta alle modalità di attuazione dei provvedimenti sovranazionali in materia, in specie della direttiva 2013/40/UE relativa agli attacchi contro i sistemi di informazione, della direttiva 713/2019/UE relativa alla lotta contro le frodi e falsificazioni degli strumenti di pagamento diversi dai contanti e della

[9] ESER A., *Comparative criminal law,* cit., p. 51.
[10] PICOTTI L., SALVADORI I., *National legislation implementing the Convention on Cybercrime*, cit., p. 5 ss.
[11] HILGENDORF E., *Zur Einführung,* cit., p. 16.

normativa europea antiriciclaggio. In questo modo sarà possibile verificare se è stata raggiunta l'auspicata armonizzazione penale nell'ambito del diritto penale dell'informatica ed, eventualmente, ipotizzare come il quadro giuridico europeo potrebbe essere migliorato per garantire l'integrazione europea, superare gli attriti tra le legislazioni nazionali e aiutare i Paesi dell'UE a mantenere una legislazione nazionale adeguata per affrontare la criminalità informatica e che al contempo sia chiara, comprensibile ed efficace.

1.1. Il contrasto alla criminalità patrimoniale e informatica in Germania: inquadramento generale

Il sistema tedesco dei reati contro il patrimonio è imperniato sulla distinzione tra delitti contro la proprietà (*Eigentumsdelikte*), detti anche delitti contro il patrimonio in senso ampio (*Vermögensdelikte im weiteren Sinn*), e delitti contro il patrimonio, detti anche delitti contro il patrimonio in senso stretto (*Vermögensdelikte im engeren Sinn*)[12]. Va però evidenziato che, a differenza di quanto avviene nel codice penale italiano, nello *Strafgesetzbuch* non esistono sezioni separate per gli *Eigentumsdelikte* e *Vermögensdelikte*. Infatti, con riferimento ai reati contro il patrimonio, nello *Strafgesetzbuch* manca una struttura sistematica nella quale i singoli reati abbiano una collocazione coordinata[13]. Le formulazioni degli elementi dei singoli reati, e di conseguenza la loro collocazione, sono il risultato di una specifica storia dei reati stessi, non l'espressione di un concetto di politica criminale concettualmente e teleologicamente coerente[14]. Addirittura, tra i reati contro il patrimonio ve ne sono alcuni che neppure trovano le proprie origini nel diritto penale patrimoniale, basti pensare alla truffa, strettamente correlata con i reati di falsificazione[15].

La distinzione tra *Eigentumsdelikte* e *Vermögensdelikte* si basa sull'oggetto della tutela, perché oggetto degli *Eigentumsdelikte* sono le cose[16] e valori patrimoniali specifici come altri diritti reali, diritti di appropriazione, diritti di credito[17]. I diritti tutelati in questa sede vengono considerati nel loro aspetto meramente giuridico-formale, secondo prospettive

[12] EISELE J., *Strafrecht Besonderer Teil. Eigentumsdelikte und Vermögensdelikte*, VI ed., Stuttgart, 2021, p.1 ss.; MAURACH R. et al., *Strafrecht Besonderer Teil. Teil I Persönlichkeits- und Vermögenswerte*, XI ed., Heidelberg, 2019, p. 392 ss.
[13] BUSCH R., *Die systematische Behandlung der sog. Vermögensdelikte im kommenden Strafrecht*, in *Zstw*, 1937, vol. 56, p. 676 ss., p. 676.
[14] KINDHÄUSER U., *Abhandlungen zum Vermögensstrafrecht*, cit., p. 18 s.
[15] *Ibid*., p. 19.
[16] MAIWALD M., *Der Zueignungsbegriff im System der Eigentumsdelikte*, Heidelberg, 1970, p. 117.
[17] LAMPE E., *Eigentumsschutz im Künftigem Strafrecht*, in H. Müller-Dietz (a cura di), *Strafrechtdogmatik und Kriminalpolitik*, Köln, 1971, p. 59 ss., p. 67 ss.

rigorosamente giuscivilistiche[18]. Ai fini della configurazione delle varie ipotesi di reato rileva essenzialmente l'impedimento del potere di disposizione, per cui in linea di principio non è necessario che il titolare del diritto subisca effettivamente alcun danno, inteso in una dimensione economica[19], dato che il pregiudizio è già presupposto dalla stessa legge[20]. La caratteristica degli *Eigentumsdelikte* è data dall'estremo formalismo cui è improntata la loro dommatica, poiché essi tutelano il concetto di proprietà intesa in senso formale[21], anche se non manca chi sottolinea che in realtà ciò che viene tutelato non è il diritto di proprietà formale in sé, ma piuttosto le possibilità di agire che da esso derivano[22]. Al contrario, nei *Vermögensdelikte* in senso stretto viene tutelato il patrimonio nel suo complesso, non le singole posizioni giuridiche in sé considerate[23]. Tale categoria, dunque, ricomprende tutto ciò che resta fuori dell'ambito di tutela degli *Eigentumsdelikte*. Per quanto anche i *Vermögensdelikte* in senso ampio si dirigano contro definite posizioni giuridiche, è decisivo per la loro configurazione che essi facciano diminuire il valore globale del patrimonio[24].

Anche questa classificazione con riferimento all'oggetto del reato non ha incontrato il favore della dottrina tedesca, che ancora oggi la ritiene insoddisfacente e incongruente[25]. Nel corso del tempo sono state elaborate diverse soluzioni nel tentativo di trovare una diversa classificazione più soddisfacente. In particolare, tra le tante ipotesi formulate, vi è chi ha proposto di mantenere ferma la distinzione tra *Eigentums- und Vermögensdelikte*, ma conferendole un'articolazione più complessa, ovvero distinguendo ulteriormente tra reati contro diritti reali (*dingliche Rechte*), reati contro diritti di appropriazione (*Zueignungsrechte*), reati contro diritti di credito (*Forderungsrechte*) e, ancora, tra reati contro il patrimonio in generale (*Vermögen überhaupt*)[26]. Altri, invece, hanno proposto di distinguere tra reati contro la proprietà (*Eigentumsverbrechen*), reati contro i diritti di appropriazione, diritti di credito e di garanzia (*Anengnungs- Forderungs und*

[18] KINDHÄUSER U., *Abhandlungen zum Vermögensstrafrecht*, Baden-Baden, 2018, p. 20.; RHEINECK B., *Zueignungsdelikte und Eigentümertineresse*, Berlin, 1979, p. 14 s. e 128 s.
[19] EISELE J., *Strafrecht Besonderer Teil*, p. 2.
[20] RHEINECK B., *Zueignungsdelikte*, cit., p. 15.
[21] HIRSCHBERG R., *Der Vermögensbegriff im Strafrecht. Versuch eines Systems er Vermögensdelikte*, Berlin, 1934, 20 ss. e 277; CRAMER P., *Vermögensbegriff und Vermögensschaden im Strafrecht*, Bad Homburg, 1968, p. 72 s.; GALLAS W., *Der Betrug als Vermögensdelikt*, in P. Bockelmann, W. Gallas (a cura di), *Festschrift für Eberhard Schmidt zum 70. Geburtstag*, Göttingen, 1961, p. 401 ss., p. 402.
[22] LICHTENTHÄLER S., *Besitzverbot und Eigentumsschutz*, Tübingen, 2020, p. 163.
[23] KINDHÄUSER U., *Abhandlungen zum Vermögensstrafrecht*, cit., p.
[24] HIRSCHBERG R., *Der Vermögensbegriff im Strafrecht*, cit., p. 20 ss.
[25] KINDHÄUSER U., *Abhandlungen zum Vermögensstrafrecht*, cit., p. 22.
[26] VON LISTZ F., SCHMIDT E., *Lehrbuch des deutschen Strafrechts*, Berlin, 1927, p. 606 ss.

Sicherungsrechte) e reati contro il patrimonio nel suo complesso (*gesamtes Vermögen*)[27]. Sono poi state elaborate proposte di distinzione basate sulla condotta, in particolare tra reati di danneggiamento (*Schädigungsdelikte*) e reati di arricchimento (*Bereicherungsdelikte*)[28], mentre altri ancora hanno distinto tra reati di sottrazione patrimoniale (*Vermögensentziehungsdelikte*) e reati di perpetuazione di altro reato (*Perpetuierungsdelikte*)[29]. Nessuna di queste proposte, tuttavia, è stata accolta.

La struttura e la classificazione dei reati contro il patrimonio in senso lato hanno avuto notevole rilevanza per il successivo sviluppo del diritto penale dell'informatica. Infatti, inizialmente la dottrina penalistica tedesca cercò di delimitare strutturalmente la criminalità da computer collocandola nel campo della criminalità economica[30]. Tale tesi fu seguita dallo stesso legislatore tedesco, tant'è che le prime fattispecie in materia di criminalità da computer vennero inserite nello *Strafgesetzbuch* con la "Seconda legge per la lotta contro la criminalità economica" (*Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität (2. WiKG)* e furono collocate accanto alle fattispecie tradizionali a tutela del patrimonio. Infatti, la nuova truffa mediante computer di cui al §263a StGB fu ricompresa tra i *Vermögensdelikte*, analogamente alla truffa comune[31]. Tra gli *Eigentumsdelikte* furono comprese le disposizioni a tutela dell'integrità dei dati, ovvero i §§ 303a, 303b dello *Strafgesetzbuch*[32], accanto al danneggiamento tradizionale. Va però evidenziato che però ad oggi la dottrina tedesca nega che i dati possano essere oggetto di proprietà, sia perché immateriali, sia perché i dati personali appartengono alla sfera più intima dell'individuo e non possono essere oggetto di trasferimento in senso proprio[33]. Tuttavia, si evidenzia anche che nella categoria "*Eigentum*" rientra non solo il diritto di proprietà in senso stretto, ma comprende tutte le manifestazioni dei diritti reali, tra cui il diritto all'uso, alla fruizione e al possesso[34]. Per questo motivo, inizialmente si ritenne che il bene giuridico tutelato dalle due

[27] WEZEL H., *Das Deutsche Strafrecht. Eine systematische Darstellung*, XI ed., Berlin, 1969 (ristampa 2011), p. 339 ss.
[28] BINDING K., *Lehrbuch des Gemeinen Deutschen Strafrechts*, cit., p. 237 ss.
[29] OTTO H., *Die Struktur des strafrechtlichen Vermögensschutzes*, Berlin, 1970, p. 87 ss.
[30] SIEBER U., *Computerkriminalität und Strafrecht*, Köln, 1977, p. 188; TIEDEMANN K., *Wirtschaftsstrafrecht und Wirtschaftskriminalität*, vol. II *Besonderer Teil*, Reinbek bei Hamburg, 1976, p. 149 s. Per approfondire v. PICOTTI L., *Studi di diritto penale dell'informatica*, cit., p. 16 ss.
[31] HAFT F., *Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität (2. WiKG). Teil 2: Computerdelikte*, in *NStZ*, 1987, p. 6 ss., p. 10.
[32] HILGENDORF E., VALERIUS B., *Computer- und Internetstrafrecht. Ein Grundriss*, Heidelberg, 2012, p. 159.
[33] KILIAN W., *Property Rights und Datenschutz*, in W.A. Kaal, M. Schmidt e A. Schwartze (a cura di), *Festschrit zu Ehren von Christian Kirchner*, Tübingen, 2014, p. 901 ss., p. 904.
[34] *Ibid*., 904.

norme fosse la proprietà «*nella sua manifestazione specializzata di dati*»[35]. Il delitto di cui al §202a, invece, fu collocato nel titolo quindicesimo relativo alla tutela relativo ma anche in questo caso inizialmente si ritenne che anche in questo caso il bene giuridico tutelato fosse il patrimonio[36], anche se ad oggi, come si esaminerà in seguito, viene privilegiata un'interpretazione differente[37].

In seguito, la delimitazione della criminalità da computer quale rigido appannaggio della criminalità economica si rivelò troppo rigida e si comprese che la criminalità informatica non poteva essere ristretta alle sole aggressioni aventi rilievo patrimoniale, in quanto i nuovi fenomeni criminosi offendono una più vasta gamma di interessi[38]. In ogni caso, attraverso la novella legislativa del 1982 furono introdotte nuove fattispecie dirette a colpire molte delle più importanti manifestazioni della criminalità da computer, tra cui la truffa mediante computer, lo spionaggio di dati, la falsificazione di dati rilevanti ai fini probatori, ecc. che verranno esaminate nel prosieguo[39]. Ulteriore nota positiva è che in Germania, a differenza che in Italia, a seguito dell'introduzione di specifici reati contro la criminalità informatica sono cominciate anche le raccolte dei dati statistici relativi alla criminalità informatica, nei quali sono indicate il numero e lo stato delle denunce pervenute annualmente all'Autorità pubblica con riferimento ai singoli reati[40].

Altra importante riforma legislativa sistematica in materia di criminalità informatica fu attuata nel 2007, per garantire la riservatezza, l'integrità e la disponibilità di dati e sistemi rispetto alle nuove minacce cibernetiche che nel tempo avevano fatto la loro comparsa[41]. Dunque, con la l. 11 agosto 2007 n. 1786 (*Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität*), che ad oggi costituisce l'ultima vera e propria riforma di sistema, sono state modificate diverse previsioni legislative quali, ad esempio, il § 202a StGB relativo

---

[35] HAFT F., *Das Zweite Gesetz*, cit., p. 10.
[36] *Ibid*.
[37] KARGL W., *sub StGB § 202a Ausspähen von Daten*, in U. Kindhäuser, U. Neumann, U. Paeffgen (a cura di), *Strafgesetzbuch. III Band*, V ed., Baden-Baden, 2017, Rn. 3.
[38] Addirittura lo stesso Sieber smentì la tesi da lui stesso prima sostenuta (v. nota 30) e in seguito evidenziò che «*Die in den lezten Jahren zu beobachtende Ausdehnung des Computermißbrauchs auf verschiedene mit der Vermögen nicht in Beziehung stehende Bereiche spricht für eine derartige Erweiterung des Begriffs der „Computerkrimialität" auf alle vorsätzlichen (strafbaren oder strafwürdigen), in einem Sachzusammenhang mit den Daten der EDV stehenden Delikte*» (L'espansione dell'uso improprio dei computer avvenuta negli ultimi anni in vari settori non correlati al patrimonio, rende evidente la necessità di estendere il concetto di "criminalità informatica" a tutti i reati dolosi (punibili o meritevoli di pena) che presentano un collegamento fattuale con i dati informatici), v. SIEBER U., *Computerkriminalität und Strafrecht*, Köln, 1980, p. 2/139.
[39] Per approfondire in merito alla genesi delle norme contro la criminalità informatica in Germania v. PICOTTI L., *Studi di diritto penale dell'informatica*, cit., p. 39 ss.
[40] SIEBER U. (a cura di), *Information Technology Crime. National Legislations and International Initiatives*, in ID (a cura di), *Ius Informationis. European series on Information Law*, vol. VI, Berlin, 1994, p. 199.
[41] GRÖSELING N., HÖFINGER F.M., *Hacking und Computerspionage - Auswirkungen des 41. StrÄndG zur Bekämpfung der Computerkriminalität*, in *MMR*, 2007, p. 549 ss., p. 549.

allo spionaggio di dati (*Ausspähen von Daten*), ed aggiunte ulteriori norme, ovvero il § 202b StGB che punisce l'intercettazione di dati (*Abfangen von Daten*), ed il § 202c StGB che punisce gli atti preparatori allo spionaggio ed all'intercettazione di dati (*Vorbereiten des Ausspähens und Abfangens von Daten*)[42]. Anche negli anni successivi il legislatore tedesco si è dimostrato molto attento alle esigenze di prevenzione e sanzione dei nuovi fenomeni criminosi, quali ad esempio il *cybercrime-as-a-service*, per cui, come si esaminerà nel prosieguo, ha emanato ulteriori riforme, che però si sono limitate ad introdurre singole disposizioni fattispecie incriminatrici, quali ad es. la ricettazione di dati di cui al §202d StGB o il nuovo §127 StGB (v. *infra* par. 7), o a modificare in misura minore quelle esistenti, senza però intervenire in maniera sistematica.

Inoltre, va evidenziato che ad essersi dimostrato particolarmente sensibile alle esigenze di tutela derivanti dall'utilizzo delle nuove tecnologie non è stato esclusivamente li legislatore tedesco, ma anche la stessa *Bundesverfassungsgericht*, la quale ha espressamente riconosciuto l'esistenza di due nuovi diritti fondamentali nati dalla diffusione delle moderne tecnologie. Il primo è il diritto fondamentale all'autodeterminazione informativa (*Grundrecht auf informationelle Selbstbestimmung*) di cui all'art. 1 co. 1 in combinato disposto con l'art. 2 co. 1 della *Grundgesetz für die Bundesrepublik Deutschland (GG)*, che consiste nella facoltà della persona di decidere per sé in merito alla divulgazione e all'uso dei propri dati personali, nonché di decidere quando ed entro quali limiti divulgare i fatti personali propria della vita[43]. Il secondo è il diritto alla garanzia della riservatezza e dell'integrità dei sistemi informatici (*Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*), che anch'esso trova il suo fondamento nell'art. 2 co. 1 in combinato disposto con l'art. all'art. 1 co. 1 della *GG*[44].

Per quanto riguarda il recepimento delle direttive europee in materia di criminalità informatica rilevanti ai fini dell'analisi in oggetto, il legislatore tedesco ha provveduto a

---

[42] PICOTTI L., SALVADORI I., *National legislation implementing the Convention on Cybercrime*, cit., p. 7. Per una prima analisi delle modifiche legislative apportate dalla l. n. 1786/2007 v. ERNST S., *Das neue Computerstrafrecht*, in *NJW*, n. 37, 2007, p. 2661 ss.

[43] BVerfG sentenza 15 dicembre 1983 - 1 BvR 209, 269, 362, 420, 440, 484/83, per approfondire v. KENJI-KIPKER D., *Informationelle Freiheit und staatliche Sicherheit. Rechtliche Herausforderungen moderner Überwachungstechnologien*, Tübingen, 2016, p. 8 ss.; FRIEDEWALD M., LAMLA J., ROßNAGEL A. (a cura di), *Informationelle Selbstbestimmung im digitalen Wandel*, Wiesbaden, 2017, *passim*; ALBERS M., *Informationelle Selbstbestimmung*, Baden-Baden, 2005, p. 151 ss.

[44] BVerfG sentenza 27 febbraio 2008 – 1 BvR 370/07 und 1 BvR 595/07; per approfondire v. HERRMANN C., *Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*, Frankfurt am Main, 2010, *passim*; SACHS M., KRINGS T., *Das neue "Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme"*, in JuS, 2008, p. 481 ss.; HIRSCH B., *Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*, in *NJW*, 2008, p. 822 ss.

recepire sia la direttiva 2018/1673/UE relativa alla lotta al riciclaggio mediante il diritto penale, sia la direttiva 713/2019/UE contro le frodi e le falsificazioni di pagamento di strumenti diversi dai contanti. Per quanto riguarda la prima direttiva menzionata, come si esaminerà nel prosieguo (v. *infra* par. 8), la legge di attuazione ha provveduto a modificare in modo significativo la disciplina penale tedesca in materia di riciclaggio. Per quanto riguarda, invece, l'attuazione della direttiva 713/2019/UE contro le frodi e le falsificazioni di pagamento di strumenti diversi dai contanti, il legislatore tedesco ha ritenuto che la disciplina in quel momento vigente fosse in gran parte conforme alle indicazioni della direttiva[45]. Dunque, l'intervento legislativo si è limitato ad ampliare l'oggetto dei reati di contraffazione di carte di pagamento, assegni e cambiali (§152a StGB, il cui titolo di reato è stato modificato in "*Fälschung von Zahlungskarten, Schecks, Wechseln und anderen körperlichen unbaren Zahlungsinstrumenten*") e di contraffazione di carte di pagamento con funzione di garanzia (§ 152b StGB – *Fälschung von Zahlungskarten mit Garantiefunktion*) e ad introdurre due nuovi reati che sanzionano rispettivamente gli atti preparatori al furto e all'appropriazione indebita di carte di pagamento, assegni, cambiali e altri strumenti fisici di pagamento diversi dai contanti (§ 152c StGB - *Vorbereitung des Diebstahls und der Unterschlagung von Zahlungskarten, Schecks, Wechseln und anderen körperlichen unbaren Zahlungsinstrumenten*) e alla frode informatica (§ 263a Abs. 3). Per quanto riguarda la direttiva 2013/40/UE relativa agli attacchi contro i sistemi di informazione, invece, la relazione presentata al progetto di legge per l'attuazione della stessa[46] ha evidenziato che la legge tedesca già soddisfaceva quasi completamente i requisiti stabiliti dalla menzionata direttiva e, dunque, la relativa legge di attuazione, ovvero la *Gesetz zur Bekämpfung der Korruption* del 20 novembre 2015, si è limitata ad aumentare la pena massima prevista per il reato di cui al § 202c StGB.

1.2. Segue: in Spagna

Il codice penale spagnolo adottato con la *Ley Orgánica* 10/1995 del 23 novembre regola i delitti contro il patrimonio nel suo titolo XIII, intitolato «*Delitos contra el patrimonio y contra el orden socioeconómico*». Analogamente a quanto avvenuto

[45] *Deutscher Bundestag Drucksache 19/25631* del 5 gennaio 2021, *Gesetzentwurf der Bundesregierung Entwurf eines Gesetzes zur Änderung des Strafgesetzbuches – Umsetzung der Richtlinie (EU) 2019/713 des Europäischen Parlaments und des Rates vom 17. April 2019 zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln und zur Ersetzung des Rahmenbeschlusses 2001/413/JI des Rates*, disponibile online al sito https://www.bmj.de

[46] *Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes zur Bekämpfung der Korruption*, Drucksache 18/4350, p. 16, disponibile *online* all'indirizzo https://www.bundestag.de/drucksachen.

nell'ordinamento italiano, anche il legislatore spagnolo ha ritenuto di sostituire la previgente rubrica "dei delitti contro la proprietà" con la nuova "delitti contro il patrimonio e l'ordine socio-economico". Tale titolo è stato ampliato includendovi anche i delitti contro l'ordine socioeconomico, al fine di ricomprendervi nuove figure delittuose sanzionatorie di nuove forme di criminalità economica che in precedenza non erano regolate[47]. Il raggruppamento in questione è stato oggetto di critiche da parte della dottrina, sia perché raggruppa figure di reato che non hanno nulla in comune, sia perché non ha specificato cosa debba intendersi per "delitti contro l'ordine socio-economico"[48]. In ogni caso, già prima del cambio della rubrica si distingueva tra due gruppi di delitti, ovvero le infrazioni di carattere collettivo con una proiezione socioeconomica, nel quale venivano incluse le norme penali sul fallimento, i delitti contro la proprietà industriale, i reati finanziari ecc., e i delitti il cui bene giuridico tutelato è costituito dal patrimonio di singoli individui, quali il furto, la frode, ecc.[49].

Nonostante la riunione di queste due sottocategorie in un unico titolo, permane una differenza tra i due gruppi, anche se la loro regolazione non segue un ordine sistematico[50]. Se da un lato l'utilizzo della locuzione "delitti contro il patrimonio" è stata accolta favorevolmente, si è però evidenziato che la stessa merita un'ulteriore precisazione, perché vi sono reati che ledono il diritto di proprietà sulle cose (ad esempio il furto e il danneggiamento), mentre altri che recano pregiudizio al patrimonio in modo differente, come ad esempio la truffa o l'estorsione[51].

---

[47] SUÁREZ GONZÁLEZ C., *Delitos contra el patrimonio y contra el orden socioeconómico*, in G. Rodriguez Mourullo (dir.), A. Jorge Barreiro (coord.), *Comentarios al código penal*, Madrid, 1997, 674 ss., p. 674 s. QUINTERO OLIVARES G., *Delitos contra el patrimonio y contra el orden socioeconómico*, in G. Quintero Olivares (dir.), J.M. Valle Muñiz (coord.), *Comentarios a la Parte Especial del Derecho Penal*, Pamplona, 1996, p. 441 ss., p. 442 evidenzia che la ragione di tale scelta non appare esplicita e che la stessa probabilmente è stata dettata dalla difficoltà di stabilire quali delitti dovessero essere ricompresi tra quelli contro il patrimonio e quali tra quelli contro l'ordine socioeconomico.

[48] Così ZUGALDIA ESPINAR J.M., *Los delitos contra la propriedad, el patrimonio y el orden socioeconomico en el nuevo codigo penal. Consideraciones generales sobre el Título XIII del N.C.P.*, in *Cuadernos de política criminal*, 1996, n. 59, p. 417 ss., p. 418. Similmente anche PRIETO DEL PINO A.M., *Criminal offences against property and against the social-economic order in Spain: a global overview and a detailed approach to some particularly relevant issues*, in *Philia journal of Judicial Studies*, 2022, vol. 1, p. 82 ss., p. 83, che ritiene che il legislatore spagnolo abbia adottato un criterio sin troppo restrittivo per la nozione di "ordine socio-economico", escludendovi senza motivo i reati fiscali nonché i reati edilizi, collocati in titoli autonomi.

[49] ROBLEDO VILLAR A., *Delitos contra el Patrimonio y el Orden socioeconómico. Comentarios a los articulos 234 a 289 del nuevo Código Penal*, Barcelona, 1997, p. 9.

[50] ALONSO PÉREZ F., *Delitos Contra el Patrimonio y contra el orden socioeconómico. Aspectos penales y criminológicos*, Madrid, 2003, p. 55; ROBLEDO VILLAR A., *Delitos contra el Patrimonio*, cit., p. 9.

[51] BACIGALUPO ZAPATER E., *Falsedad documental, estafa y administración desleal*, Madrid, 2007, p. 156. *Contra* ZUGALDIA ESPINAR J.M., *Los delitos contra la propriedad, el patrimonio y el orden socioeconómico*, cit., p. 421 ss., il quale sostiene che il legislatore abbia errato a raggruppare i delitti contro la proprietà assieme a quelli contro il patrimonio, dato che i primi non richiedono necessariamente la realizzazione di un danno al patrimonio della vittima.

A differenza del codice penale italiano, i reati contro il patrimonio non sono espressamente suddivisi in macrocategorie, ma vengono suddivisi in microcategorie nei singoli capitoli, quali ad esempio "*De la extorsión*", "*De las defraudaciones*" o "*De los daños*". Alcuni autori, però, distinguono tra *delitos de apropriación* e *delitos patrimoniales*. La distinzione consiste nel fatto che nel primo caso la lesione della proprietà si produce per il solo fatto dell'avvenuta espropriazione (*expropriación*) della cosa, per cui è indifferente che la cosa sia priva di valore economico o che la perdita economica sia stata successivamente ripianata. Nel *delito patrimonial*, invece, si richiede la causazione o comunque l'intenzione di causare un pregiudizio patrimoniale[52]. Nell'ambito di quest'ultimo gruppo si distingue a loro volta tra *delitos de apoderamiento* e *defraudatorios*: nel primo caso la cosa viene ottenuta contro la volontà del proprietario o del possessore, mentre nel secondo caso la lesione patrimoniale viene ottenuta mediante la cooperazione artificiosa della vittima[53]. Tra i delitti contro l'ordine socioeconomico, invece, si trova oggi anche il riciclaggio di denaro[54].

Peculiarità dell'ordinamento spagnolo è che, nel caso di commissione di una pluralità di reati contro il patrimonio, la disciplina del reato continuato è diversa rispetto a quella ordinaria. L'art. 74 c.p., infatti, che regola il *delito continuado*, al co. 2 prevede che se si tratta di reati contro il patrimonio la pena dev'essere determinata tenendo conto del pregiudizio totale arrecato[55].

Neppure il *Código penal* spagnolo contiene una definizione generale di patrimonio ai fini del diritto penale, per cui anche in questo caso vi è stato un intenso dibattito in merito

[52] SUÁREZ GONZÁLEZ C., *Delitos contra el patrimonio*, p. 676.
[53] MUÑOZ CONDE F., *Derecho Penal. Parte Especial*, XXIII ed., Valencia, 2021, p. 392 s.; HERRERO HERRERO C., *Infracciones penales patrimoniales*, Madrid, 2000, p. 50.
[54] GONZÁLEZ RUS J.J., *Los delitos contra el patrimonio*, in B. Del Rosal Blasco (a cura di), *Estudios sobre el nuevo Código Penal de 1995*, Valencia, 1997, p. 180.
[55] Il *delito continuado* è regolato all'art. 74 c.p. e non è che *fictio iuris* che consente di considerare come unico reato molteplici azioni od omissioni che di per se stesse già costituirebbero un reato consumato o tentato. Analogamente al reato continuato previsto nel codice penale italiano, prevede il cumulo giuridico delle pene per il caso della commissione di più azioni od omissioni in esecuzione del medesimo disegno criminoso o approfittando di un'identica occasione. Tuttavia, si differenzia dall'omologo italiano sia perché la norma in questione specifica espressamente che le azioni od omissioni possono aver cagionato un'offesa ad una o più persone, sia, soprattutto, perché il reato continuato è applicabile soltanto nel caso della violazione di uno stesso precetto penale o precetti della "stessa natura" o di "natura analoga". Dunque, la norma impone che le fattispecie violate tutelino beni giuridici omogenei. Va poi evidenziato che l'art. 74.3 c.p. prevede l'inapplicabilità della disciplina del reato continuato nel caso in cui ad essere lesi siano "beni strettamente personali", ad eccezione dei delitti contro l'onore, la libertà sessuale e l'indennità sessuale. Sul punto cft. CHOCLÁN MONTALVO J.A., *El delito continuado*, Madrid, 1997, p. 179 ss.; CUERDA RIEZU A., *Concurso de delitos y determinación de la pena*, Madrid, 1992, p. 97 ss.; CASTIÑERA PALOU M., *El delito continuado*, Barcelona, 1977, p. 29 ss.; MUÑOZ CONDE F., GARCÍA ARÁN M., *Derecho Penal. Parte General*, X ed., Valencia, 2019, p. 446; MIR PUIG S., *Derecho Penal. Parte General*, X ed., Barcelona, 2015, p. 670 s.

al contenuto del concetto di tale concetto[56]. Anche qui è prevalsa la concezione mista giuridico-economica di patrimonio, che reputa come essenziale per la valutazione del danno non tanto il saldo negativo che deriva dalla diminuzione e accrescimento di singole parti dal patrimonio, bensì la diminuzione della disponibilità economica del titolare del patrimonio[57] (v. *supra* cap. I, par. 1). Oggetto di un delitto contro il patrimonio possono essere solo quei beni dotati di un valore economico, che possono essere una cosa materiale, un diritto, un bene mobile o immobile[58]. Dunque, rientrano nella nozione di patrimonio non solo i diritti reali, ma anche le obbligazioni[59], per cui per pregiudizio patrimoniale si intendono tutte le diminuzioni economicamente valutabili[60]. Si ritiene poi che per essere soggetto passivo di un delitto contro il patrimonio non sia sufficiente una relazione meramente di fatto con la cosa, ma occorra la presenza di una relazione tutelata dall'ordinamento giuridico.

Per quanto riguarda specificamente lo sviluppo del diritto penale dell'informatica, anche in questo caso, analogamente a quanto avvenne in Germania, tale settore venne inizialmente considerato come una mera manifestazione della criminalità economica[61]. Inizialmente la dottrina spagnola non ritenne che i delitti informatici costituissero un gruppo autonomo e omogeneo, bensì un ambito di rischio derivante dall'espansione dell'utilizzo delle tecnologie informatiche, da punire in base alle fattispecie vigenti oppure da introdurre *ex novo*, sulla base delle fattispecie tradizionali esistenti[62]. Tale tesi ha influenzato il legislatore. Infatti, nonostante il *Código penal* spagnolo sia stato emanato in epoca molto più

---

[56] Per approfondire v. per tutti PASTOR MUÑOZ N., *La determinación del engaño típico en el delito de estafa*, cit., p. 32 ss.

[57] ALONSO PÉREZ F., *Delitos Contra el Patrimonio*, cit., p. 27. Sul punto v. PASTOR MUÑOZ N., *La determinación del engaño típico en el delito de estafa*, cit., p. 38 s. e 82 ss.

[58] ANTÓN ONECA J., voce *Estafa*, in C.E. Mascareñas (a cura di), *Nueva Enciclopedia jurídica*, vol. XI, Barcelona, 1975, p. 57 ss., p. 68; GONZÁLEZ RUS J.J., *Los intereses económicos de los consumidores. Protección penal*, Madrid, 1986, cit., p. 258.

[59] MUÑOZ CONDE F., *Derecho Penal. PE*, cit., p. 390.

[60] Sul punto v. Tribunal Supremo, sez. I penale, sentenza 23 aprile 1992, n. 20999, secondo cui «*sin embargo, en la Doctrina moderna el concepto personal de patrimonio, según el cual el patrimonio constituye una unidad personalmente estructurada, que sirva al desarrollo de la persona en el ámbito económico, ha permitido comprobar que el criterio para determinar el daño patrimonial en la estafa no se debe reducir a la consideración de los componentes objetivos del patrimonio. El juicio sobre el daño, por el contrario, debe hacer referencia también a componentes individuales del titular del patrimonio. Dicho de otra manera: el criterio para determinar el daño patrimonial es un criterio objetivo-individual. De acuerdo con éste, también se debe tomar en cuenta en la determinación del daño propio de la estafa la finalidad patrimonial del titular del patrimonio. Consecuentemente, en los casos en los que la contraprestación, no sea de menor valor objetivo, pero implique una frustración de aquella finalidad, se debe apreciar también un daño patrimonial*».

[61] DE LA MATA BARRANCO N. J., *Delitos contra los sistemas de información*, in N.J. De la Mata Barranco, J. Dopico Gómez-Aller, J.A. Lascuraín Sánchez, A. Nieto Martín (a cura di), *Derecho penal económico y de la empresa*, Madrid, 2018, p. 727 ss., p. 727; ALONSO PÉREZ F., *Delitos Contra el Patrimonio*, cit., p. 53 ss.

[62] RUIZ VADILLO E., *Tratamiento de la delincuencia informática como una de las expresiones de la criminalidad económica*, in *PJ*, num. speciale IX, 1989, p. 53 ss., 56 s.; GUTIÉRREZ FRANCÉS M.L., *Fraude informático y estafa*, Madrid, 1991, p. 61; ROMEO CASABONA C.M., *Poder informático y seguridad jurídica*, Madrid, 1987, p. 42.

recente rispetto allo *Strafgesetzbuch* tedesco e al codice penale italiano, quando già si erano diffusi comportamenti delinquenziali indotti dallo sviluppo delle nuove tecnologie informatiche, neppure esso contiene un titolo autonomo dedicato ai reati informatici. Anzi, le condotte volte a reprimere le manifestazioni criminose espressione della c.d. criminalità informatica non furono neppure collocate in fattispecie autonome, come invece è avvenuto in Italia e in Germania, ma inizialmente furono incorporate nelle fattispecie tradizionali, come avvenne, ad esempio, nel caso della frode informatica e del danneggiamento informatico, tramite la c.d. tecnica dell'assimilazione del tipo, equiparando le peculiarità del sistema informatico agli oggetti ed elementi già previsti nelle fattispecie tradizionali[63].

Va però evidenziato che la Costituzione spagnola, a differenza di quella italiana e tedesca, all'art. 18.4 specificamente riconosce la protezione necessaria rispetto alle intrusioni informatiche dei dati che possono affliggere l'intimità personale o familiare dei cittadini. Dunque, in questo caso la stessa disposizione costituzionale evidenzia come le tecnologie informatiche siano non solo uno strumento socialmente utile, ma rappresentino anche una potenziale occasione di lesione dell'intimità personale e familiare dei cittadini, per cui il loro utilizzo dev'essere limitato, o comunque disciplinato, dalla legge, al fine di garantire il pieno esercizio dei propri diritti, da parte dei cittadini stessi[64].

Anche il sistema spagnolo è stato oggetto di diverse riforme nel corso degli anni, anche per apportare gli adeguamenti richiesti dal diritto sovranazionale. A tal proposito, va menziona la *Ley Orgánica* n. 15/2003 del 25 novembre 2003 con la quale è stata introdotta la punibilità degli atti preparatori alla truffa mediante computer. Tuttavia, la prima riforma legislativa sistematica che ha riguardato anche la criminalità informatica fu attuata con la *Ley orgánica* 5/2010 del 22 giugno 2010. Tale legge è stata introdotta allo scopo di dare attuazione alla Decisione quadro 2005/222/JAI, ma non alla Convenzione *cybercrime*[65]. Attraverso tale novella legislativa fu inserito l'art. 248.2 lett. c) c.p. al fine di sanzionare la frode informatica commessa attraverso l'utilizzo di carte di credito, in conformità alla Decisione quadro 2005/222/JAI (oggi sostituita dalla direttiva 2013/40/UE), nonché l'art. 399-*bis* c.p. relativo alla falsificazione di carte di credito. Fu poi inserito all'art. 197.3 c.p. il reato di accesso abusivo a sistema informatico o telematico, oltre a nuove disposizioni in materia di danneggiamenti informatici, con l'aggiunta di ulteriori condotte a quelle già

[63] CHOCLÁN MONTALVO J.A., *Estafa por computación y criminalidad económica vinculada a la informática*, in *Actualidad penal*, 1997, n. 47, p. 1068 ss., p. 1076.
[64] PLANTAMURA V., *La tutela penale delle comunicazioni informatiche e telematiche*, cit., p. 848.
[65] SALVADORI I., *Los nuevos delitos informáticos en el Código penal español con la Ley Orgánica 5/2010. Perspectiva de derecho comparado*, in *ADPCP*, 2011, vol. 64, p. 221 ss., p. 250.

sanzionate, nonché di una circostanza aggravante per il fatto commesso nell'ambito di un'organizzazione criminale e la limitazione della punibilità ai soli casi in cui il danno causato sia "grave"[66].

Per quanto riguarda il recepimento delle direttive europee in materia di criminalità informatica rilevanti ai fini dell'analisi in oggetto, la direttiva 2013/40/UE relativa agli attacchi contro i sistemi di informazione è stata attuata con la *Ley Orgánica* 1/2015 del 30 marzo 2015, con la quale furono introdotti in nuovi artt. 197 *bis* e 197 *ter* c.p., che sanzionano rispettivamente l'accesso abusivo al sistema informatico e l'intercettazione di dati[67], nonché gli artt. 264 *bis* e 264 *ter* c.p., che sanzionano rispettivamente il sabotaggio informatico e gli atti preparatori alla commissione di un danneggiamento informatico. Anche la direttiva 2018/1673/UE del 23 ottobre 2018 sulla lotta al riciclaggio mediante il diritto penale è stata recentemente attuata con la *Ley Orgánica* 6/2021 del 28 aprile 2021, con la quale è stata aggiunta una nuova circostanza aggravante al reato di riciclaggio (*blanqueo*). La direttiva 2019/713/UE sulla frode e falsificazione dei mezzi di pagamento diversi dai contanti, invece, è stata appena recepita dalla nuova *Ley Orgánica* 14/2022, del 22 dicembre 2022, la quale ha modificato in modo significativo le fattispecie di frode informatica, falsificazione ed indebito utilizzo degli strumenti di pagamento diversi dai contanti.

2. La rilevanza penale degli atti preparatori alla commissione di più gravi reati *lato sensu* patrimoniali

In Germania il sistema della punibilità degli atti preparatori è sostanzialmente incentrato sul § 202c StGB, reato di pericolo astratto[68] che punisce gli atti preparatori diretti alla commissione di un delitto di spionaggio o di intercettazione di dati[69] (*Vorbereiten des*

[66] DE URBANO CASTRILLO E., *Los delitos informáticos tras la reforma del CP de 2010*, in *Delincuencia Informática. Tiempos de Cautela y Amparo*, Cizur Menor, 2012, p. 17 ss., p. 20 ss.

[67] Il co. 1 consiste in una trasposizione del previgente art. 197.3 c.p., che con la riforma la condotta ivi descritta divenne fattispecie autonoma, mentre l co. 2 richiama la previgente disposizione dell'art. 197.1 c.p., v. DE LA MATA BARRANCO N. J., *Delitos contra los sistemas de información*, cit., p. 731.

[68] WEIDEMANN M., *sub StGB § 202c Vorbereiten des Ausspähens und Abfangens von Daten*, in B. Von Heintschel-Heinegg (Hrsg), *Beck-Online Kommentar StGB*, LIII ed., München, 2022, Rn. 3.; ERNST S., *Das neue Computerstrafrecht*, cit., p. 2663.

[69] «*(1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er 1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder 2.Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft*» ((1) Chiunque prepara la commissione di un reato ai sensi della sezione 202a o della sezione 202b producendo, acquisendo per sé o un'altra persona, vendendo, fornendo a un altro, diffondendo o rendendo altrimenti accessibili: 1. password o altri codici di sicurezza che consentono l'accesso ai dati (§ 202a Abs. 2), o 2. programmi informatici il cui scopo è la commissione di tali reati, è punito con la reclusione non superiore a due anni o con la pena pecuniaria).

Ausspähens und Abfangens von Daten). Inoltre, per effetto del richiamo di cui ai §§303a Abs. 3 e 303b Abs. 5 StGB, il delitto in questione punisce anche gli atti preparatori ai delitti di alterazione di dati e sabotaggio informatico.

Tale norma incriminatrice, introdotta con l. 11 agosto 2007 n. 1786, sanziona le condotte di produzione, acquisizione, vendita, fornitura, diffusione di *password* o codici d'accesso (oltre alla loro pubblicazione sul *web*) o programmi informatici allo scopo di commettere spionaggio o intercettazione di dati[70]. L'elemento soggettivo di tale reato, dunque, è il dolo, che può essere anche eventuale[71]. Oggetto del reato, invece, sono le *password*, nelle quali vengono ricomprese anche gli identificativi, formando un'unità per l'accesso[72], e i programmi informatici. In questi ultimi sono ricompresi i c.d. *hacker-tools*[73]. Si è, però, posto il problema relativo alla punibilità dei *software* c.d. *dual-use* (v *supra* cap. II par. 1). Si è evidenziato, infatti, che strumenti quali i c.d. *sniffer*, che monitorano, registrano e analizzano il traffico all'interno di una rete non vengono appositamente progettati per commettere reati, poiché sono comunemente utilizzati per eliminare gli errori o ottimizzare il traffico di dati[74]. Sul punto si è pronunciata la Corte costituzionale tedesca, la quale ha statuito che oggetto del reato di cui al § 202c StGB può essere solamente un programma il cui scopo è la commissione di un reato ai sensi dei §§ 202a o 202b StGB, per cui dev'essere stato sviluppato o modificato con l'intenzione di utilizzarlo per commettere i reati citati. Inoltre, questa intenzione deve essersi manifestata oggettivamente. Dunque, non è sufficiente che un programma, come nel caso dei cosiddetti strumenti a duplice uso, sia semplicemente idoneo o addirittura particolarmente adatto alla commissione dei reati informatici specificati[75]. Tuttavia, anche per non restringere in maniera eccessiva il campo applicativo della fattispecie, si è in seguito evidenziato che non è necessario che il programma sia destinato esclusivamente alla commissione di un reato informatico, bensì è sufficiente che lo scopo oggettivo dello strumento sia anche la commissione di tale reato[76].

[70] ERNST S., *Das neue Computerstrafrecht*, cit., p. 2662.
[71] WEIDEMANN M., *sub StGB § 202c*, cit., Rn. 9.
[72] KOCHHEIM D., *Cybercrime und Strafrecht*, cit., p. 299. In tale nozione rientra anche il PIN per l'accesso al sistema di *home banking*, in tal senso ALTENHAIN K., *StGB § 202c Vorbereiten des Ausspähens und Abfangens von Daten*, in H. Matt, J. Renzikowski (a cura di), *Strafgesetzbuch*, II ed., München, 2020, Rn. 2.
[73] WEIDEMANN M., *sub StGB § 202c*, cit., Rn. 6.
[74] HILGENDORF E., VALERIUS B., *Computer- und Internetstrafrecht*, cit., p. 172; ERNST S., *Das neue Computerstrafrecht*, cit., p. 2663
[75] BverfG, ordinanza del 18 maggio 2009 – 2 BvR 2233/07, 2 BvR 1151/08, 2 BvR 1524/08.
[76] WEIDEMANN M., *sub StGB § 202c*, cit., Rn. 7.

Vi è, invece, chi propone di non concentrarsi sulle caratteristiche oggettive del programma, ma su criteri soggettivi, in particolare sull'uso che dello stesso viene fatto[77].

Per quanto riguarda le modalità di aggressione al patrimonio che rientrano nell'ambito applicativo della norma in questione, pacificamente si ritiene che tale fattispecie sanzioni la prima fase dei *phishing attacks*, ovvero l'illecita apprensione delle credenziali altrui, o comunque il furto d'identità in senso lato (*Identitätsdiebstahl*)[78]. Non è idonea, però, a sanzionare il mero invio delle *mail* di *phishing*, dato che, in mancanza di espressa previsione legislativa, trattandosi di delitto, il tentativo non è punibile[79].

Tale fattispecie, dunque, può dirsi analoga all'art. 615-*quater* c.p., anche se, a differenza di quest'ultimo, non sanziona il mero possesso degli oggetti ivi indicati. Altro parallelismo con l'art. 615-*quater* c.p. è che, come quest'ultimo, il § 202c StGB è reato perseguibile d'ufficio, mentre i reati di spionaggio e intercettazione di dati non lo sono[80].

Per quanto riguarda l'ordinamento spagnolo, fattispecie omologa al § 202c StGB è costituita dall'art. 197 *ter código penal*, che sanziona le condotte prodromiche all'accesso abusivo al sistema informatico e all'intercettazione di dati, nonché al trattamento di dati non autorizzato[81]. Come sopra evidenziato, tale norma fu introdotta dalla *Ley Orgánica* 1/2015 per dare attuazione alla direttiva 2013/40/UE sugli attacchi diretti contro i sistemi di informazione, anticipando così la soglia di rilevanza penale[82]. La formulazione di tale norma è quasi identica a quella di cui all'art. 7 della menzionata direttiva. Infatti, oggetto del reato in questione sono: alla lettera a) un programma informatico progettato o specificamente adattato per commettere uno dei reati elencati dalla norma, mentre alla lettera b) una *password*, un codice di accesso o "dati simili" che consentono l'accesso a tutto o parte di un sistema informatico. Analogamente al § 202c StGB, la norma stessa richiede che il programma informatico sia concepito o specificamente adattato per commettere uno dei reati ivi elencati, ovvero l'accesso abusivo al sistema informatico, l'intercettazione di dati,

---

[77] NESTLER N., *Hacker-Tools im StGB*, in *JURA*, 2021, n. 6, p. 629 ss., p. 637; HILGENDORF E., VALERIUS B., *Computer- und Internetstrafrecht*, cit., p. 172.
[78] BORGES G., SCHWENK J., STUCKENBERG C., WEGENER C., *Identitätsdiebstahl*, cit., p. 233.
[79] MARBERTH-KUBICKI A., *Computer- und Internetstrafrecht*, München, 2010, p. 63.
[80] HILGENDORF E., VALERIUS B., *Computer- und Internetstrafrecht*, cit., p. 171.
[81] «*Será castigado con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses el que, sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los apartados 1 y 2 del artículo 197 o el artículo 197 bis: a) un programa informático, concebido o adaptado principalmente para cometer dichos delitos; o*
b) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información».
[82] MORALES PRATS F., *La reforma de los delitos contra la intimidad artículo 197 CP*, in G. Quintero Olivares (a cura di), *Comentario a la reforma penal de 2015*, Cizur Menor, 2015, p. 459 ss., p. 466.

telecomunicazioni, nonché il trattamento illecito dei dati personali (art. 197.1 e 197.2 e 197 *bis* c.p.). Anche in questo caso, la dottrina ha criticato l'introduzione di tale requisito, che ricalca la formula usata nell'art. 7 della direttiva 2013/40/UE, evidenziato le difficoltà nello stabilire quando i programmi informatici siano costruiti o adattati principalmente per commettere i suddetti reati[83].

La fattispecie in questione sanziona la produzione, l'acquisizione per l'uso, l'importazione o comunque la fornitura a terzi degli oggetti di cui alle lettere a) e b). Dunque, a differenza che nel novellato art. 615-*quater* c.p., non è sanzionato il mero possesso di tali strumenti, condotta di cui, si rammenta, la direttiva 2013/40/UE non richiedeva obbligatoriamente la punibilità. Trattasi di norma a più fattispecie, per cui le condotte ivi descritte sono tra loro alternative[84]. Analogamente all'art. 615-*quater* c.p., è stato evidenziato che le condotte ivi descritte sono in realtà neutre e non esprimono di per sé un disvalore, per cui l'elemento soggettivo assume importanza fondamentale[85]. Infatti, per quanto riguarda quest'ultimo, anche in questo caso, analogamente all'art. 615-*quater* c.p., è previsto che il reo agisca con un determinato fine, ovvero l'intenzione di facilitare la commissione di uno dei delitti elencati dalla norma. La fattispecie richiede poi che soggetto agente agisca senza essere specificamente autorizzato, ovvero senza il consenso di colui che può disporne o senza autorizzazione prevista dalla legge[86].

La fattispecie in questione pone alcuni problemi con riferimento al concorso di reati. Essa, infatti, è punita con la stessa identica pena del reato di cui all'art. 197 *bis* c.p., che sanziona l'accesso abusivo al sistema informatico o l'intercettazione di dati, per cui non vi può essere consunzione del primo reato in quest'ultimo, altrimenti si arriverebbe alla soluzione paradossale di punire più gravemente colui che si procura la *password* rispetto a colui che dopo essersela procurata provi ad accedere al sistema senza però riuscirci[87]. La dottrina ritiene, pertanto, che tra i due reati si debba applicare il *principio de alternatividad*[88],

[83] MORALES PRATS F., *La reforma de los delitos contra la intimidad artículo 197 CP*, cit., p. 466.
[84] GALÁN MUÑOZ A., *Los ciberdelitos en el ordenamiento español*, Barcelona, 2019, p. 127.
[85] MORALES PRATS F., *La reforma de los delitos contra la intimidad artículo 197 CP*, cit., p. 467.
[86] GALÁN MUÑOZ A., *Los ciberdelitos*, cit., p. 127.
[87] *Ibid*., 130.
[88] Il codice penale spagnolo regola espressamente il concorso apparente di norme all'art. 8, il quale, a differenza dell'art. 15 del codice penale italiano, menziona espressamente tra i criteri guida non solo il principio di specialità, ma anche quello di sussidiarietà, di consunzione e di alternatività (*alternatividad*). Quest'ultimo è formulato nell'apt. 4 dell'art. 8 c.p., secondo cui «*en defecto de los criterios anteriores, el precepto penal más grave excluirá los que castiguen el hecho con pena menor*». Per MUÑOZ CONDE F., GARCÍA ARÁN M., *Derecho Penal. PG*, cit., p. 450 s. il criterio in questione serve per evitare casi di impunità o pene spropositate nei casi in cui vi sia una cattiva coordinazione delle diverse fattispecie penali con struttura simile. Secondo MIR PUIG S., *Derecho Penal. Parte General*, cit., p. 687, invece, l'unico caso in cui non sono applicabili i criteri anteriormente elencati, ovvero specialità, sussidiarietà e consunzione, è nel caso in cui per un errore o

con applicazione a quest'ultimo caso del reato di cui all'art. 197 *ter* c.p. e non (il tentativo di) quello posteriormente commesso.

Peculiarità dell'ordinamento spagnolo è la previsione di una circostanza aggravante di cui all'art. 197-*quater* c.p. per i fatti commessi «*en el seno de una organización o grupo criminal*», anch'essa introdotta dalla *Ley Orgánica* 1/2015. Tale circostanza aggravante è particolarmente appropriata perché permette di sanzionare più gravemente la raccolta di credenziali e dati bancari effettuata su larga scala da associazioni a delinquere. Quanto al concetto di organizzazioni criminali, si deve fare riferimento all'art. 570-*bis*.2 c.p.[89], che la definisce come "l'insieme formato da più di due persone in modo stabile o per un tempo indeterminato, che in modo concertato e coordinato si dividono vari compiti o funzioni allo scopo di commettere reati".

A differenza di quanto accade nell'ordinamento tedesco, e analogamente a quello italiano, gli atti preparatori al danneggiamento e al sabotaggio informatico sono sanzionati in modo autonomo dall'art. 264-*ter código penal*, anch'esso introdotto dalla *Ley Orgánica* 1/2015. Con l'introduzione di questa norma, dunque, si è colmata una lacuna sussistente nell'ordinamento evidenziata dalla dottrina[90]. Tale reato punisce chiunque allo scopo di commettere un danneggiamento di dati o di sistemi informatici produce, acquisisce per l'uso, importa o mette altrimenti a disposizione di terzi un programma per computer specificamente adattato allo scopo oppure una *password*, un codice d'accesso o dati simili che consentono l'accesso al sistema informatico[91]. La formulazione di tale norma ricalca quella di cui all'art. 7 della direttiva 2013/40/UE[92] ed è quasi identica a quella di cui al menzionato art. 197-*ter código penal*, dato che le condotte sanzionate e l'oggetto del reato

una disattenzione del legislatore due o più norme sanzionino esattamente lo stesso fatto. V. anche CASTELLÓ NICÁS N., *El concurso de normas penales*, Granada, 2000, p. 115 ss.; GARCÍA ALBERO R., *"Non bis in Idem" material y concurso de leyes penales*, Barcelona, 1995, p. 321 ss.

[89] DEL VALLE SIERRA LÓPEZ M., *Los delitos de descubrimiento y revelación de secretos en el Código Penal de 2015: artículos 197,197 bis,197 ter, 197 quáter, 197 quinquies y 198*, in J. Del Carpio Delgado (a cura di), *Algunas Cuestiones de Parte Especial tras la Reforma de 2015 del Código Penal*, Valencia, 2018, p. 132 ss., p. 182.

[90] FLORES PRADA I., *Criminalidad informática*, cit., p. 187; MATA Y MARTÍN R.M., *Delincuencia informática y derecho penal*, cit., p. 70.

[91] «*Será castigado con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses el que, sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los dos artículos anteriores: a) un programa informático, concebido o adaptado principalmente para cometer alguno de los delitos a que se refieren los dos artículos anteriores; o b) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información*».

[92] ANDRÉS DOMÍNGUEZ A. C., *Reformas en daños*, in G. Quintero Olivares (a cura di), *Comentario a la reforma penal del 2015*, cit., p. 548.

sono identici[93]. L'unica differenza risiede nel dolo specifico[94], perché in questo caso si richiede il fine di commettere un danneggiamento informatico. È evidente la sua similitudine con l'art. 615-*quinquies* c.p., anche se neppure in questo caso si punisce la mera detenzione. Nell'ambito applicativo della norma in questione rientra pertanto la creazione o la diffusione di programmi informatici progettati specificamente per infettare un *computer* al fine di prenderne il controllo da remoto e causarne il blocco[95].

2.1. Le norme in materia di contraffazione.

Per quanto riguarda le *e-mail* di *phishing* o i siti contraffatti al fine di indurre gli utenti a fornire dati personali e/o credenziali o invogliarli a cliccare su un *link* contenente *malware*, un'ulteriore norma rilevante nell'ordinamento tedesco è il § 269 StGB, che punisce la falsificazione di dati rilevanti ai fini probatori (*Fälschung beweiserheblicher Daten*)[96]. Come sopra evidenziato, tale norma fu introdotta nello *Strafgesetzbuch* già con la *2. WiKG*. Tale fattispecie non riguarda la tutela delle genuinità dei documenti cartacei, anzi, la previsione legale richiede espressamente che i dati non siano materialmente percepibili[97] e ciò consente la sua applicazione anche e soprattutto all'universo virtuale. Inoltre, nel concetto di "giuridicamente rilevanti" (*Beweiserheblichkeit*) sono ricomprese anche le *e-mail* o le informazioni false relative al mittente e ai dati di connessione, nella misura in cui questi vengono utilizzati in *Internet* per qualsiasi azione rilevante dal punto di vista giuridico[98]. Si è, infatti, escluso che la norma preveda una qualche forma di previa certificazione di

[93] GALÁN MUÑOZ A., *Los ciberdelitos en el ordenamiento español*, Barcelona, 2019, p. 198.
[94] Nell'ordinamento spagnolo, a differenza che in quello italiano, non esiste una definizione generale di delitto doloso. In questo caso si distingue tra dolo intenzionale (*dolo directo de primer grado*), diretto (*dolo directo de segundo grado*) ed eventuale (*dolo eventual*). Il fine criminoso richiesto dalla norma viene qualificato come *elemento subjectivo del tipo* doloso, ovvero tutti quei requisiti di carattere soggettivo diversi dal dolo che la fattispecie di reato richiede. V. DÍEZ RIPOLLÉS J.L., *Los elementos subjetivos del delito. Bases metodológicas*, Buenos Aires, 2007, *passim*; LAURENZO COPELLO P., *Dolo y conocimiento*, Valencia, 1999, *passim*; nella manualistica v. MIR PUIG S., *Derecho Penal. PS*, cit., p. 286; MUÑOZ CONDE F., GARCÍA ARÁN M., *Derecho Penal. PS*, cit., p. 263.
[95] GALÁN MUÑOZ A., *Los ciberdelitos*, cit., p. 200 s.
[96] «*(1) Wer zur Täuschung im Rechtsverkehr beweiserhebliche Daten so speichert oder verändert, daß bei ihrer Wahrnehmung eine unechte oder verfälschte Urkunde vorliegen würde, oder derart gespeicherte oder veränderte Daten gebraucht, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft*» ((1) Chiunque immette o modifica i dati destinati a fornire prova nel traffico giuridico al fine di inganno, in modo tale che nel caso di loro utilizzo ne resulterebbe un documento non autentico o falsificato o utilizzi i dati memorizzati o modificati in questa maniera, è punito con la reclusione non superiore a cinque anni o con un'ammenda).
[97] PUPPE I., SCHUMANN K., *sub. StGB § 269 Fälschung beweiserheblicher Daten*, in U. Kindhäuser, U. Neumann, H. Ullrich Paeffgen (Hrsg.), *Strafgesetzbuch*, München, V ed., 2017.
[98] WEIDEMANN M., *sub StGB § 269 Fälschung beweiserheblicher Daten*, in B. Von Heintschel-Heinegg (Hrsg), *Beck-Online Kommentar StGB*, XLVII ed., München, 2020.

autenticità dei dati tutelati[99]. Il reato in questione richiede però che le *e-mail* mediante le quali si realizza il *phishing* contengano un messaggio chiaro e che i falsi mittenti corrispondano a soggetti realmente esistenti, perché la disposizione in questione ha una funzione di garanzia nei confronti degli operatori nel traffico giuridico[100]. Tale fattispecie, quindi, non si configura quando gli indirizzi dei mittenti corrispondono a nomi di fantasia o il messaggio contenga errori o alterazioni del logo tali da farlo apparire come falso grossolano. Si può, ritenere, però, che lo *spoofing*, ovvero la tecnica utilizzata per mascherare indirizzi mail e numero di telefono rientri nell'ambito applicativo del § 269 StGB[101].

Va poi evidenziato che qualora il *phisher* nella creazione delle *mail* e dei siti truffaldini utilizzi nomi, loghi, scritte o il dominio di una banca si può configurare anche la responsabilità penale ai sensi del § 143 della *Markengesetz*, che vieta l'uso di segni identici o simili a loghi o marchi altrui[102]. Non solo, ma è pure ipotizzabile una responsabilità penale ai sensi dei del § 106 della *Gesetz über Urheberrecht und verwandte Schutzrechte*, ovvero la legge sul diritto d'autore e sui diritti connessi, qualora il reo nella progettazione del sito abbia utilizzato segni grafici e decorativi che possono essere classificati come "opera" (*Werk*)[103].

La dottrina maggioritaria tedesca non ritiene invece applicabile la diversa fattispecie della contraffazione di documenti (*Urkundenfälschung* § 267 StGB)[104] alle *e-mail* di *phishing* o ai siti di *pharming* che imitano in tutto, anche nel logo, quelli degli istituti di credito o altre istituzioni pubbliche: infatti, a differenza della falsificazione di dati giuridicamente rilevanti, in tale norma si richiama il concetto di "documento", che richiede che i caratteri siano "visibili", ovvero che i segni che incorporano il pensiero siano materialmente percepibili, non essendo sufficiente la possibilità della loro visualizzazione[105].

---

[99] HÖINIGHAUS N., *Der hypothetische Vergleich des §269 StGB unter Berücksichtigung der tatsächlichen und normativen Vergleichbarkeit von Schrifturkunde und moderner (Computer-) Datenurkunde*, Stuttgart, 2005, p. 181.
[100] GRAF J.P., *"Phishing"*, cit., p. 132.
[101] MARBERTH-KUBICKI A., *Computer- und Internetstrafrecht*, cit., p. 56.
[102] HANSEN D., *Strafbarkeit des Phishing nach Internetbanking-Legitimationsdaten*, Hamburg, 2007, p. 124 ss.
[103] *Ibid*.
[104] «*(1) Wer zur Täuschung im Rechtsverkehr eine unechte Urkunde herstellt, eine echte Urkunde verfälscht oder eine unechte oder verfälschte Urkunde gebraucht, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft*». ((1) Chiunque, a fini di inganno nel traffico giuridico, confeziona un documento non autentico, falsifica un documento autentico o utilizza un documento non autentico o falsificato, è punito con la reclusione non superiore a cinque anni o con una multa).
[105] STUCKENBERG C.F., *Zur Strafbarkeit von "Phishing"*, cit., p. 885; Sul concetto di documento v. anche JAKOBS G., *Urkundenfälschung*, Köln, 2000, p. 8.

La giurisprudenza è concorde con quest'opinione[106].

Anche la dottrina spagnola si è interrogata in merito all'applicabilità delle fattispecie tradizionali di falso alla creazione di siti di *phishing* o allo *spoofing*. Per quest'ultimo, in particolare, non essendovi nel *código penal* spagnolo una fattispecie che sanzioni espressamente il furto d'identità, si è discusso in merito all'applicabilità del delitto di usurpazione dello stato civile di cui all'art. 401 c.p.[107]. Essa, però, viene generalmente esclusa, poiché la norma in questione richiede che lo stato civile venga "usurpato", dunque, si richiede una certa continuità nell'usurpazione dell'identità, non l'invio di semplici *mail*[108]. L'art. 401 c.p., però, trova sicuramente applicazione nei casi di *online dating scam* e simili, nei casi in cui i criminali utilizzino le generalità di persone realmente esistenti per creare finti profili *social*[109]. Qualora, però, nei casi di *phishing* classico, il reo si finga un'istituzione pubblica, tale condotta potrà integrare il diverso reato di cui all'art. 402 c.p., che sanziona l'usurpazione delle funzioni pubbliche e l'intromissione, perché in questo caso non vi è richiesta la continuità sopra menzionata[110]. Tuttavia, tale reato potrà essere integrato solo se il reo, oltre ad attribuirsi carattere ufficiale, compia anche atti propri di un'autorità o di un pubblico ufficiale. Per altri autori ancora, la falsa creazione di siti di *phishing* può integrare il reato di falsità in documento commerciale di cui all'art. 392 c.p.[111]. A tal proposito, va evidenziato che la giurisprudenza del *Tribunal Supremo* ha ritenuto che il concetto di documento commerciale (*documento mercantil*) abbia portata amplia, comprensiva di qualsiasi documento che sia espressione di un'operazione commerciale, espressa nella creazione, modifica o estinzione di obblighi di natura commerciale, sia che serva a cancellarli o ad accreditare diritti o obblighi di tale natura. Tali documenti, dunque, non solo quelli espressamente disciplinati dal Codice del Commercio o dalle Leggi Commerciali, ma anche tutti quelli che registrano un'operazione commerciale o sono validi o efficaci per registrare diritti o obblighi di tale natura o servono a dimostrarli[112]. Tuttavia, la stessa

[106] OLG Hamburg: *Beschluss v.* 06.11.2012 - 1 Ss 134/11, in *LSK*, 2013, p. 120775 ss.
[107] MIRÓ LLINARES F., *La respuesta penal al ciberfraude. Especial atención a la responsabilidad de los muleros del phishing*, in *RECPC*, n. 15-12, p. 12:1 ss., p. 17.
[108] MIRÓ LLINARES F., *La respuesta penal al ciberfraude*, cit., p. 19; FLORES MENDOZA F., *Respuesta penal al denominado robo de identidad en las conductas de phishing bancario*, in *EPC*, 2014, vol. 34, p. 301 ss., p. 311.
[109] SERRANO FERRER M.P., *Derecho penal y nuevas tecnologías*, Cizur Menor, 2021, p. 121.
[110] MIRÓ LLINARES F., *La respuesta penal al ciberfraude*, cit., p. 19.
[111] VELASCO NÚÑEZ E., *Fraudes informáticos en Red: del* phishing *al* pharming, in *LL*, 2007, n. 37, p. 57 ss., p. 61.
[112] Tribunal Supremo, sez. I penale, sentenza 22 giugno 2006, n. 788; Tribunal Supremo, sez. I, sentenza 20 novembre 2008, n. 764; Tribunal Supremo, sez. I, sentenza 8 maggio 1997, n. 625; Tribunal Supremo, sez. I, sentenza 18 ottobre 2004, n. 1148.

giurisprudenza ha precisato che l'art. 392 c.p. cit. si riferisce unicamente a quei documenti commerciali che meritano una protezione speciale, perché la loro materialità incorpora una presunzione di veridicità e autenticità equivalente a un documento pubblico[113]. Per altri autori, dunque, siti di *phishing* o gli indirizzi ID non possono essere ricompresi nella nozione di *documentos mercantiles*, in quanto gli stessi non hanno uno speciale valore probatorio[114].

Per quanto riguarda l'applicabilità dei reati di falso, va evidenziato che nel fornire la nozione di documento valida ai fini penali, l'art. 26 *código penal* si riferisce a "qualsiasi supporto materiale che incorpori dati con rilevanza giuridica", per cui include al suo interno sia il documento elettronico, sia il supporto informatico[115]. Vi è, dunque, chi ritiene che il sito di *phishing* rientri nell'ambito applicativo del reato di falsità in documento privato di cui all'art. 395 c.p.[116]. Altri autori, tuttavia, lo escludono, perché l'art. 26 *código penal* richiede che i dati in questione abbiano "efficacia probatoria o qualsiasi altro tipo di rilevanza giuridica", requisito che difficilmente una semplice pagina *web* possiede[117].

2.2. Gli atti preparatori alla falsificazione e indebito utilizzo di strumenti di pagamento diverso dai contanti.

Nell'ordinamento tedesco altre norme rilevanti ai fini della punibilità degli atti preparatori sono i §§ 152c StGB, che punisce gli atti preparatori diretti al furto e all'appropriazione indebita di carte di pagamento, assegni, cambiali e altri strumenti fisici di pagamento diversi dai contanti (*Vorbereitung des Diebstahls und der Unterschlagung von Zahlungskarten, Schecks, Wechseln und anderen körperlichen unbaren Zahlungsinstrumenten*) e il 263a Abs. 3, che sanziona la preparazione del reato di truffa mediante computer (*Vorbereitung eines Computerbetrugs*). Il primo è stato introdotto *ex novo* dalla *Einundsechzigste Gesetz zur Änderung des Strafgesetzbuches* di attuazione della direttiva 2019/713/UE, mentre il secondo è stato modificato da quest'ultima. Nell'ordinamento spagnolo, invece, gli atti preparatori alla falsificazione di strumenti di

[113] Tribunal Supremo, sez. I penale, sentenza 22 giugno 2006, n. 788. Per la dottrina v. NIETO MARTÍN A. *Falsedades en la Empresa*, in N.J. De la Mata Barranco, J. Dopico Gómez-Aller, J.A. Lascuraín Sánchez, A. Nieto Martín (a cura di), *Derecho penal económico y de la empresa*, p. 685 ss., p. 701.
[114] MIRÓ LLINARES F., *La respuesta penal al ciberfraude*, cit., p. 20.
[115] MIRÓ LLINARES F., *Cibercrímenes económicos y patrimoniales*, en I. Ortiz De Urbina Gimeno (a cura di), *Memento práctico penal y económico de la empresa 2011-2012*, Madrid, 2011, p. 469 ss., p. 483. V. Anche BACIGALUPO ZAPATER E., *Falsedad documental*, cit., p. 60 e 20, che evidenzia come «*lo esencial del contenido de un documento es la corporización de una declaración del pensamiento de una persona*».
[116] AGUADO LÓPEZ S., ORTIZ NAVARRO J.F., CABEDO VILLAMÓN F., *Instrucción y enjuiciamiento de los modernos fraudes informáticos*, in C. Sanchis Crespo (a cura di), *Fraude electrónico. Su gestión penal y civil*, Valencia, 2015, p. 101 ss., p. 109.
[117] MIRÓ LLINARES F., *La respuesta penal al ciberfraude*, cit., p. 20.

pagamento e alla frode informatica sono sanzionati rispettivamente agli artt. 400 e 249.2 lett. a) c.p. Il primo è presente sin dalla formulazione originaria del codice, anche se è stato oggetto di modifiche da parte della *Ley Orgánica* 1/2015 e dalla recentissima *Ley Orgánica* 14/2022, mentre il secondo è stato inserito dalla *Ley Orgánica* 15/2003 del 25 novembre 2003 ed oggi, a seguito dell'ultima *Ley Orgánica* 14/2022, è collocato nel novellato art. 249.2 lett. a) c.p.

Il § 152c StGB sanziona alcuni atti preparatori alla commissione di un furto o un'appropriazione indebita che abbiano per oggetto carte di credito e strumenti di pagamento fisici non in contanti[118]. Oggetto di reato sono i programmi, i dispositivi informatici, *password* o codici di sicurezza il cui scopo sia la commissione di furti o appropriazioni indebite al fine di ottenere carte di pagamento nazionali o estere, assegni, cambiali o altri strumenti di pagamento fisico non in contanti. A tal proposito, il legislatore stesso ha precisato che i programmi e i dispositivi informatici devono essere stati progettati principalmente per la commissione di reati finalizzati all'ottenimento di strumenti di pagamento rilevanti o adattati specificamente a tale scopo[119]. Quest'interpretazione, dunque, si conforma ai già citati *Considerando* n. 10 e 16 della direttiva 2019/713/UE sulla necessità di evitare di criminalizzare gli strumenti di pagamento diversi dai contanti, qualora questi ultimi siano prodotti e posti in commercio per fini legittimi. Nell'ambito applicativo della norma in questione, dunque, rientrano dispositivi collegati agli sportelli bancomat per rubare la carta inserita dal cliente[120]. Invece, per quanto riguarda le *password* e i codici di sicurezza, il legislatore ha riconosciuto che gli stessi non sono generalmente prodotti o progettati per scopi specifici, per cui ha ritenuto opportuno richiedere l'idoneità di questi mezzi di offesa per la commissione del reato[121]. Tuttavia, va osservato che difficilmente una *password* o un codice possono servire a commettere un furto o un'appropriazione indebita di carte fisiche

[118] «*Wer eine Straftat nach § 242 oder § 246, die auf die Erlangung inländischer oder ausländischer Zahlungskarten, Schecks, Wechsel oder anderer körperlicher unbarer Zahlungsinstrumente gerichtet ist, vorbereitet, indem er 1. Computerprogramme oder Vorrichtungen, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft oder einem anderen überlässt oder 2. Passwörter oder sonstige Sicherungscodes, die zur Begehung einer solchen Tat geeignet sind, herstellt, sich oder einem anderen verschafft oder einem anderen überlässt, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft*» (Chiunque prepari la commissione di un reato ai sensi del § 242 o del § 246 che sia finalizzato all'ottenimento di carte di pagamento nazionali o estere, assegni, cambiali o altri strumenti fisici di pagamento non in contanti 1. producendo, procurando per sé o per altri, o consegnando ad altri programmi o dispositivi informatici il cui scopo è la commissione di uno di tali reati; o 2. producendo, procurando per sé o per altri o consegnando a un'altra persona, password o altri codici di sicurezza idonei alla commissione di uno di tali reati, è punito con la pena detentiva fino a due anni o con la pena pecuniaria).

[119] *Deutscher Bundestag Drucksache 19/25631*, cit., p. 23.

[120] WEIDEMANN M., *sub StGB § 152c* in B. von Heintschel-Heinegg (a cura di), *Beck Online Kommentar Strafgesetzbuch*, cit., Rn. 6.

[121] *Deutscher Bundestag Drucksache 19/25631*, cit., p. 23.

materiali e, soprattutto, ancor più raro è che gli stessi soddisfino il requisito di idoneità oggettiva richiesto dal legislatore tedesco. Va poi evidenziato che si tratta di reato preparatorio ai reati di furto e appropriazione indebita, i quali, come si esaminerà meglio nel prosieguo, hanno necessariamente quale oggetto del reato una cosa materiale (*Sache*), per cui è evidente che la preparazione deve servire all'asportazione fisica della carta, non semplicemente alla sua clonazione. Non si comprende, però, tale scelta, dato che le carte di credito non vengono quasi più fisicamente rubate, bensì ne vengono utilizzati i relativi codici. Peraltro, per rubare fisicamente una carta di credito non si devono certo utilizzare dispositivi informatici. Resta da vedere, dunque, quale sarà il campo applicativo della norma in questione.

Si ritiene che il bene giuridico tutelato dal § 152c sia, come per i §§ 242 (furto) e 246 (appropriazione indebita) StGB, la proprietà di strumenti di pagamento fisici non in contanti per garantire la sicurezza e la funzionalità delle operazioni di pagamento senza contanti[122]. Per questo motivo, la collocazione della norma accanto alle fattispecie a tutela dei mezzi di pagamento è stata contestata[123]. Tale reato viene classificato come reato di pericolo astratto[124]. Per quanto riguarda l'elemento soggettivo, trattasi di reato doloso, che può essere punito anche a titolo di dolo eventuale, ma è richiesto che l'autore agisca al fine di commettere un furto o un'appropriazione indebita di una carta di credito o di uno strumento di pagamento fisico diverso dai contanti[125].

Norma analoga è presente anche nel codice penale spagnolo, ovvero l'art. 400, che sanziona gli atti preparatori[126] alla falsificazione di una carta di credito o assegno[127]. Tale norma è stata oggetto di modifica a seguito della *Ley Orgánica* n. 1/2015 cit., con la quale

[122] WEIDEMANN M., *sub StGB § 152c*, cit., Rn. 3.
[123] *Ibid*.
[124] *Ibid*., Rn. 4.
[125] *Ibid*., Rn. 11.
[126] Va evidenziato che nel Codice penale spagnolo il tentativo implica l'inizio dell'esecuzione (v. art. 16.1 c.p., secondo cui «*hay tentativa cuando el sujeto da principio a la ejecución del delito directamente por hechos exteriores, practicando todos o parte de los actos que objetivamente deberían producir el resultado, y sin embargo éste no se produce por causas independientes de la voluntad del autor*»), per cui la stessa norma ai fini della punibilità del tentative distingue tra atti preparatori ed esecutivi. Dunque, gli atti preparatori sono generalmente non punibili, a meno che non siano specificamente sanzionati dal codice. Gli atti preparatori punibili, però, sono unicamente la *conspiración*, la *proposición* e la *provocación*. V. FARRÉ TREPAT E., *La tentativa de delito. Doctrina y jurisprudencia*, Madrid, 2011, p. 221; MIR PUIG S., *Derecho Penal. PG*, cit., p. 355; MUÑOZ CONDE F., GARCÍA ARÁN M., *Derecho Penal. PG*, cit., p. 391 ss. In lingua inglese v. GARCÍA MAGNA D., *Principals and accessories*, in A.M. Prieto del Pino (a cura di), *Lessons of Spanish Substantive Criminal Law*, vol. II, Cizur Menor, 2020, p. 121 ss., p. 126 ss.
[127] «*La fabricación, recepción, obtención, tenencia, distribución, puesta a disposición o comercialización de útiles, materiales, instrumentos, sustancias, datos y programas informáticos, aparatos, elementos de seguridad o cualquier otro medio diseñado o adaptado específicamente para la comisión de los delitos descritos en los capítulos anteriores, se castigarán con la pena señalada en cada caso para los autores*».

sono state aggiunte due nuove condotte a quelle già sanzionate (*recepción y obtención*) e modificati gli oggetti del reato, con l'aggiunta della clausola di chiusura "altri mezzi"[128], nonché dalla *Ley Orgánica* 14/2022, di attuazione della direttiva 2019/713/UE.

Oggetti del reato sono strumenti, materiali, sostanze, dati e programmi informatici, apparati, elementi di sicurezza o altri mezzi specificamente progettati o specificamente adattati alla commissione di un falso. È presente la clausola di chiusura "qualsiasi altro mezzo". A seguito della *Ley Orgánica* 14/2022 gli oggetti ivi indicati non devono più essere devono essere "specificamente destinati" alla falsificazione, requisito che secondo la giurisprudenza indicava l'attitudine e la qualità dell'oggetto di essere di utilità ai fini della commissione della falsificazione, ovvero quando non si ravvisa altra diversa utilità nello stesso[129], ma devono essere "progettati o specificamente adattati" allo scopo. In passato la giurisprudenza aveva ritenuto rientrasse nell'ambito applicativo della norma in questione la detenzione di strumenti per la fabbricazione di carte di credito contraffatte[130], escludendo dalla portata applicativa della norma in questione quegli strumenti che, pur potendo essere utilizzati per la falsificazione, non sono specificamente ad essa destinati. La dottrina, invece, riteneva che l'illegittimità di tali strumenti non dipendesse unicamente dalla loro natura oggettiva, ma anche dall'utilizzo designato dal soggetto[131]. I requisiti della progettazione o dell'adattamento specifico, però, appaiono molto più stringenti rispetto alla mera "destinazione"; pertanto sembra da escludere si possa prescindere dalla natura oggettiva degli strumenti in questione, con il conseguente problema già esaminato in materia di *dual-use software* dell'individuazione dell'obiettiva finalità dei programmi informatici.

Condotte sanzionate dalla norma sono la fabbricazione, la ricezione, l'ottenimento e la detenzione, senza che sia specificato che tali condotte debbano essere finalizzate alla commissione di uno specifico reato. Alle condotte già sanzionate la *Ley Orgánica* 14/2022 ha poi ulteriormente aggiunto la distribuzione, la messa a disposizione e la commercializzazione.

Il reato di cui all'art. 400 *Código penal* si consuma con la mera detenzione od ottenimento di tali strumenti, senza che sia necessario il loro effettivo impiego nella

[128] QUINTERO OLIVARES G., *Artículo 400*, in G. Quintero Olivares (dir.), F. Morales Prats (coord.), *Comentarios a la parte especial del derecho penal*, Cizur Menor, 2016, p. 1624 ss., p. 1625.
[129] Tribunal Supremo, sez. I penale, sentenza 30 settembre 2011 n. 988; Tribunal Supremo, sez. I penale, sentenza 9 maggio 2006 n. 567.
[130] Tribunal Supremo, sez. I penale, sentenza 27 aprile 2007, n. 392.
[131] FLORES PRADA I., *Criminalidad informática. Aspectos sustantivos y procesales*, Valencia, 2012, p. 236; QUINTERO OLIVARES G., *Artículo 400*, cit., p. 1625.

falsificazione[132]. Trattasi di reato di pericolo astratto[133] e, per quanto riguarda l'elemento soggettivo, punito a titolo di dolo, che richiede la conoscenza della specifica finalità illecita degli oggetti posseduti o fabbricati[134].

Peculiarità è che gli atti preparatori sono puniti con la stessa identica pena del reato consumato di falso[135]. Per alcuni autori la stessa pena è giustificata dal fatto che la potenzialità lesiva del comportamento ivi sanzionato è particolarmente elevata[136]. Per questo motivo, per quanto riguarda il concorso con l'eventuale successiva falsificazione, non si ritiene sia possibile operare l'assorbimento dell'art. 400 c.p. nell'ipotesi di falso, per cui vi dev'essere concorso di reati[137].

Più che al § 152c StGB, dunque, tale norma assomiglia di più al sopra esaminato art. 493-*quater* c.p. del codice penale italiano. Tuttavia, va evidenziato che la *Ley Orgánica* 14/2022 di attuazione della direttiva 2019/713/UE contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti ha aggiunto al novellato art. 249.2 lett. b) una nuova fattispecie per sanzionare specificamente il furto e l'appropriazione indebita di carte di credito, debito e qualsiasi altro mezzo materiale o immateriale di pagamento diverso dai contanti, finalizzato alla sua utilizzazione fraudolenta[138]. Anche in questo caso valgono le medesime critiche espresse con riferimento al § 152c StGB in merito all'opportunità di inserire una fattispecie che sanzioni la materiale apprensione (*sustracción*) di uno strumento immateriale di pagamento, che per la sua natura non è suscettibile di essere sottratto o comunque oggetto di impossessamento.

2.3. Gli atti preparatori alla commissione della frode informatica.

Per quanto riguarda, invece, gli atti preparatori alla frode informatica, nell'ordinamento tedesco essi sono sanzionati dal §263a Abs. 3 StGB[139]. La punibilità degli

---

[132] Tribunal Supremo, sez. I penale, sentenza 9 maggio 2008, n. 279.
[133] QUINTERO OLIVARES G., *Artículo 400*, cit., p. 1625.
[134] LASCURAÍN SÁNCHEZ J.A., *sub art. 400*, in G. Rodriguez Mourullo (ed.), Jorge Barreiro A. (coord.), *Comentarios al código penal*, Madrid, 1997, p. 1077 ss., p. 1078.
[135] FARALDO CABANA P., *Las nuevas tecnologías en los delitos contra el patrimonio y el orden socioeconómico*, Valencia, 2009, p. 289.
[136] LASCURAÍN SÁNCHEZ J.A., *sub art. 400*, cit., p. 1078.
[137] QUINTERO OLIVARES G., *Artículo 400*, cit., p. 1625; FARALDO CABANA P., *Las nuevas tecnologías*, cit., p. 291. In giurisprudenza v. Tribunal Supremo, sez. I penale, sentenza 9 maggio 2008, n. 226. *Contra* CASTELLÓ NICÁS N., *El concurso de normas penales*, cit., p. 160, secondo cui tra i due reati vi è progressione criminosa, per cui troverebbe applicazione il principio di consunzione/assorbimento.
[138] «*Los que, para su utilización fraudulenta, sustraigan, se apropiaren o adquieran de forma ilícita tarjetas de crédito o débito, cheques de viaje o cualquier otro instrumento de pago material o inmaterial distinto del efectivo*».
[139] «*(3) Wer eine Straftat nach Absatz StGB § 263A Absatz 1 vorbereitet, indem er: 1. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, feilhält,*

atti preparatori fu inserita dalla l. n. 65 del 27 dicembre 2003, di attuazione della direttiva 2001/413/CE relativa alle frodi e falsificazioni dei mezzi di pagamento diversi dai contanti. L'anticipazione della tutela penale del patrimonio è prevista unicamente per la truffa mediante computer e non anche per la truffa comune, differenza che ha suscitato critiche in dottrina per via della disparità di trattamento[140]. La norma sanziona colui che produca, procuri per sé o per altri, venda, custodisca o consegni ad altri uno degli oggetti del reato, ovvero i programmi informatici e, a seguito della *Einundsechzigste Gesetz zur Änderung des Strafgesetzbuches*, anche *password* e codici di sicurezza[141]. Per la nozione di questi ultimi si può far riferimento a quella già elaborata in relazione all'esaminato §202c StGB[142]. Se, pertanto, in passato si era esclusa l'applicabilità della norma in questione al fenomeno del *phishing* poiché i codici identificativi non erano ricompresi tra gli oggetti del reato[143], oggi, a seguito dell'ampliamento dell'oggetto del reato, questa tesi può senz'altro ritenersi superata. La norma richiede che i programmi informatici abbiano lo scopo di commettere una frode informatica ("*deren Zweck die Begehung einer solchen Tat ist"*). Anche in questo caso, dunque, si è posto il problema di come poter individuare l'obiettiva finalità di tali programmi, in particolare con riferimento ai già menzionati *software* a duplice uso[144]. A tal proposito, una parte della dottrina ha escluso che l'obiettiva idoneità possa basarsi sulla volontà d'uso dell'utente, poiché altrimenti basterebbe dichiarare di voler utilizzare quel determinato programma per andare esenti da responsabilità penale[145]. Tuttavia, la dottrina maggioritaria, preso atto dell'impossibilità di utilizzare criteri puramente oggettivi, ritiene che sia proprio la volontà dell'utente nell'utilizzare quel *software* a scopo criminale a determinarne l'oggettiva idoneità richiesta dalla norma[146]. Elemento soggettivo richiesto

verwahrt oder einem anderen überlässt oder 2.Passwörter oder sonstige Sicherungscodes, die zur Begehung einer solchen Tat geeignet sind, herstellt, sich oder einem anderen verschafft, feilhält, verwahrt oder einem anderen überlässt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft» (Chiunque prepari un reato ai sensi del par. § 263a abs. 1 StGB: 1. producendo, procurando per sé o per altri, vendendo, custodendo o consegnando ad un'altra persona programmi informatici il cui scopo è la commissione di tale reato, o 2. producendo, procurando per sé o per altri, vendendo, custodendo o consegnando ad altri *password* o altri codici di sicurezza idonei alla commissione di tale reato, è punito con la pena detentiva fino a tre anni o con una pena pecuniaria).

[140] DUGGTE S., *Vorbereitung eines Computerbetruges. Auf dem Weg zu einem „grenzlosen" Strafrecht*, in B. Heinrich (a cura di), *Festschrift für Ulrich Weber zum 70. Geburtstag*, Bielefeld, 2004, p. 285 ss., p. 296 s.

[141] SCHMIDT H.C., *sub StGB § 263a*, in B. von Heintschel-Heinegg (a cura di), *Beck Online Kommentar Strafgesetzbuch*, cit., Rn. 49.

[142] *Deutscher Bundestag Drucksache 19/25631*, cit., p. 23.

[143] HILGENDORF E., VALERIUS B., *Computer- und Internetstrafrecht*, cit., p. 158.

[144] MARBERTH-KUBICKI A., *Computer- und Internetstrafrecht*, cit., p. 41.

[145] *Ibid*.

[146] GERCHE M., BRUNST P.W., *Praxishandbuch Internetstrafrecht*, Stuttgart, 2009, p. 104; HILGENDORF E., VALERIUS B., *Computer- und Internetstrafrecht*, cit., p. 158.; SCHMIDT H.C., *sub StGB § 263a*, cit, Rn. 48.

dalla norma è il dolo, che può essere anche eventuale, ma il reo deve agire al fine di commettere una frode informatica[147]. Nel campo applicativo del §263a Abs. 3 StGB di nuova formulazione rientra, dunque, lo *skimming*[148], nonché l'installazione di *spyware*[149]. Tuttavia, questa norma ancora non è idonea a sanzionare il mero invio delle *mail* di *phishing*, perché le stesse non rientrano né nella nozione di programma informatico, né in quella di *password* o codici di sicurezza[150].

Va poi evidenziato che il §263a Abs. 2 StGB prevede la punibilità anche della frode informatica tentata, per cui si pone il problema dei rapporti tra quest'ultima fattispecie e la punibilità degli atti preparatori. Tuttavia, va evidenziato che, a differenza dell'art. 56 di cui codice penale italiano, il §22 StGB espressamente distingue tra atti preparatori ed esecutivi ai fini della punibilità del tentativo, prevedendo la punibilità solo di questi ultimi[151]. Pertanto, come ritenuto dalla giurisprudenza, si configura la truffa mediante computer nella forma tentata solo qualora il reo compia una delle azioni indicate nelle Var. da 1 a 4 del § 263a StGB, dunque, ad esempio nel caso in cui provi ad inserire una carta di credito clonata in un bancomat[152] oppure tenti di utilizzare indebitamente una carta di credito altrui provando ad indovinare la combinazione del codice PIN[153].

Anche il legislatore spagnolo sanziona gli atti preparatori alla commissione della frode informatica, all'art. 249.2 lett. a) c.p.[154]. Tale norma, introdotta con la *Ley Orgánica* n. 15/2003 del 25 novembre 2003 e modificata dalla Ley Orgánica 14/2022, sanziona le condotte di fabbricazione, importazione, ottenimento, possesso, trasporto, commercio o messa a disposizione per altri di dispositivi, strumenti, dati, programmi informatici o "qualsiasi altro mezzo" specificamente progettato o adattato per la commissione delle frodi "di cui al presente articolo". A differenza di quanto appare a prima vista, la norma in questione non sanziona una specifica modalità di preparazione del reato di frode informatica,

---

147 GERCHE M., BRUNST P.W., *Praxishandbuch Internetstrafrecht*, Stuttgart, 2009, p. 105.
148 *Deutscher Bundestag Drucksache 19/25631*, cit., p. 23.
149 SCHMIDT H.C., *sub StGB § 263a*, cit., Rn. 48.
150 MARBERTH-KUBICKI A., *Computer- und Internetstrafrecht*, cit., p. 41.
151 Per approfondire v. GROPP W., SINN A., *Strafrecht Allgemeiner Teil*, V ed., Berlin, 2020, p. 364; ROXIN C., *Strafrecht Allgemeiner Teil*, vol. II, München, 2003, p. 360; SAFFERLING C.J.M., *Die Abgrenzung zwischen strafloser Vorbereitung und strafbarem Versuch im deutschen, europäischen und im Völkerstrafrecht*, in *ZStW*, 2006, Vol. 118, n. 3, p. 682 ss.; HIRSCH H.J., *Untauglicher Versuch und Tatstrafrecht*, in *Festschrift für Claus Roxin zum 70. Geburtstag*, 2001, Berlin, p. 711 ss.; BEILING E., *Die Lehre vom Verbrechen*, Tübingen, 1906, p. 346 ss.
152 BayObLG, sez. V penale, sentenza 24 giugno 1993 - 5 St RR 5/93.
153 *Ibid*.
154 «*Los que fabricaren, importaren, obtuvieren, poseyeren, transportaren, comerciaren o de otro modo facilitaren a terceros dispositivos, instrumentos o datos o programas informáticos, o cualquier otro medio diseñado o adaptado específicamente para la comisión de las estafas previstas en este artículo*».

dato che, a differenza della sopra esaminata norma tedesca, non richiede affatto che il reo agisca al fine di commettere specificamente una frode informatica. Pertanto, secondo alcuni autori, ciò separa quest'ipotesi dal reato di frode informatica e la rende figura autonoma rispetto ad essa[155]. Peraltro, la nuova collocazione della norma in questione a seguito della *Ley Orgánica* 14/2022, ovvero in un comma diverso rispetto alla frode informatica, conferma tale tesi.

La norma prevede che i dispositivi, gli strumenti, i dati, i programmi informatici in questione siano destinati alla commissione di una *estafa* "di cui al presente articolo". Prima della modifica di cui alla *Ley Orgánica* 14/2022, quando la truffa e la frode informatica erano regolate nello stesso articolo, alcuni autori ritenevano che la norma in questione sanzionasse anche gli atti preparatori alla truffa comune, per cui fosse idonea a sanzionare anche coloro che creano i siti di *High Yield Investment Program* (v. *supra* cap. I par. 5), in quanto il sito stesso poteva essere considerato programma informatico specificamente destinato alla commissione della truffa in questione, vista la sua idoneità a fungere da strumento per reclutare i potenziali investitori/vittime, e sussiste senz'altro il dolo richiesto[156]. Altri autori, invece, sostenevano che la commissione del reato in esame dovesse considerarsi necessariamente vincolata alla commissione di una frode informatica[157]. A seguito della modifica legislativa di cui alla menzionata *Ley Orgánica* 14/2022 questa appare essere l'unica interpretazione possibile, dato che la truffa e la frode informatica sono state collocate in due norme distinte.

Per quanto riguarda le condotte sanzionate, trattasi di norma a più fattispecie, ove le condotte sono alternative tra loro[158]. Per fabbricazione si intende la creazione del programma informatico, per introduzione l'inserimento del programma in rete o nel sistema informatico, per possesso la mera detenzione o salvataggio de dati, mentre per messa a disposizione qualsiasi trasmissione del programma[159]. Le condotte di importazione, ottenimento, trasporto, commercio o la messa a disposizione "in qualsiasi modo" per altri sono state ulteriormente aggiunte dalla *Ley Orgánica* 14/2022.

---

[155] GALÁN MUÑOZ A., *Los ciberdelitos*, cit., p. 161.
[156] FERNÁNDEZ-SALINERO SAN MARTIN M.A., *Las Estafas Piramidales y Su Trascendencia Jurídico Penal*, Madrid, 2019, p. 37.
[157] SÁNCHEZ LINDE M., *Las Conductas del Artículo 248.2.B) del Código Penal como delito de estafa informática*, in C. Sanchis Crespo (a cura di), *Fraude electrónico. Su gestión penal y civil*, Valencia, 2015, p. 379 ss., p. 382 s.
[158] GALÁN MUÑOZ A., *Los ciberdelitos*, cit., p. 161.
[159] SÁNCHEZ LINDE M., *Las Conductas del Artículo 248.2.B)*, cit., p. 382 s.

Oggetto del reato sono i programmi informatici, intesi in senso lato[160], nonché, a seguito della citata *Ley Orgánica* 14/2022, anche i dispositivi, gli strumenti, i dati e "qualsiasi altro mezzo". Esattamente come avviene nel § 263a Abs. 3 StGB, anche in questo caso la norma esige che gli oggetti in questione siano progettati o specificamente adattati alla commissione di una frode informatica. Con riferimento a tale requisito, prima della modifica di cui alla menzionata *Ley Orgánica* 14/2022 era sufficiente che gli oggetti in questione fossero "specificamente destinati", per cui si riteneva necessaria un'attitudine o un'idoneità oggettiva del programma in questione, senza che rilevasse il semplice utilizzo ai fini illeciti che ne fa un soggetto[161]. Secondo alcuni autori, tuttavia, si trattava però di un requisito meramente simbolico, posto che la totalità dei programmi informatici possono avere multiple specifiche funzioni, per cui ad applicare questo requisito si rischiava di rendere la norma in questione priva di portata applicativa in concreto[162]. Nonostante ciò, con l'ultima riforma il legislatore spagnolo non ha tenuto conto di questa critica e ha notevolmente ristretto la portata applicativa della norma in questione, dato che, analogamente a quanto osservato per il novellato art. 400 c.p., il nuovo requisito non consente di prescindere dall'oggettiva finalità degli oggetti in questione.

Per quanto riguarda l'elemento soggettivo, anche in questo caso la norma è punita a titolo di dolo, che sussiste qualora l'autore sia cosciente che il programma sia specificamente destinato a e stia per essere effettivamente impiegato nella commissione di frodi informatiche[163].

Anche in questo gli atti preparatori sono sanzionati con la stessa pena prevista per la fattispecie consumata, cosa che è stata oggetto di critiche, per contrasto col principio di proporzionalità[164]. Nonostante ciò, la *Ley Orgánica* 14/2022 ha lasciato invariata l'identità della pena. Peraltro, si evidenzia che in questo modo il tentativo di frode informatica viene punito meno gravemente degli atti preparatori[165]. A tal proposito, vi è chi ritiene che il

[160] FERNÁNDEZ TERUELO J.G., *Derecho penal e internet. Especial consideracióm de los delitos que afectan a jóvenes y adolescentes*, Valladolid, 2011, p. 53
[161] GALÁN MUÑOZ A., *Los ciberdelitos*, cit., p. 162; QUINTERO OLIVARES G., *De las estafas*, in G. Quintero Olivares (dir.), F. Morales Prats (coord.), *Comentarios a la parte especial del derecho penal*, cit., p. 649 ss., p. 653.
[162] CRUZ DE PABLO J.A., *Derecho penal y nuevas tecnologías. Aspectos sustantivos. Adaptado a la reforma operada en el Código Penal por Ley Orgánica 15/2003 de 25 noviembre, especial referencia al nuevo artículo 286 CP*, Madrid, 2006, p. 46.
[163] FARALDO CABANA P., *Las nuevas tecnologías*, cit., p. 114.
[164] DOPICO GÓMEZ-ALLER J., *Estafas y otros fraudes en el ámbito empresarial*, in N.J. De la Mata Barranco, J. Dopico Gómez-Aller, J.A. Lascuraín Sánchez, A. Nieto Martín (a cura di), *Derecho penal económico y de la empresa*, cit., p. 169 ss., p. 231; CRUZ DE PABLO J.A., *Derecho penal y nuevas tecnologías*, cit., p. 46.
[165] FARALDO CABANA P., *Las nuevas tecnologías*, cit., p. 117.

programma debba essere destinato a commettere un gran numero di frodi nei confronti di un numero ampio e indeterminato di soggetti passivi, perché solo in questo modo è possibile giustificare il fatto che la pena di quest'ultimo reato è identica a quella della fattispecie consumata[166].

Nell'ambito applicativo della norma in questione rientra la detenzione di programmi *software* per realizzare il *pharming*[167], nonché *sniffer* e *keylogger*[168]. Tuttavia, per quanto riguarda questi ultimi vi è chi dubita dell'applicabilità della norma in questione, dato che gli stessi vengono progettati e installati per individuare i malfunzionamenti del sistema; dunque, non potrebbero definirsi specificamente destinati alla commissione delle frodi[169]. Anche la pagina *web* viene considerata programma informatico e, dunque, suscettibile di ricadere sotto l'ambito applicativo della norma in questione[170]. Prima della modifica di cui alla l. 14/2022 si riteneva non vi rientrasse l'invio di messaggi *spam* o comunque di *phishing*, dato che questi ultimi non possono essere considerati programmi informatici[171]. Ciò si riteneva valesse anche se questi ultimi siano portatori di programmi *malware* occulti, dato che la condotta sanzionata è quella della detenzione o messa a disposizione di programmi informatici, non l'invio di *e-mail*[172]. Tuttavia, a seguito di detta novella, in particolare dell'aggiunta "qualsiasi altro mezzo", si ritiene che tale teoria meriti di essere rivista. Per quanto riguarda i rapporti con il tentativo, anche in questo caso si esclude che l'invio della mera *e-mail* di *phishing*, nonché la sola l'infezione di *malware* o *spyware*, di per sé, possano essere considerate come tentativo di frode informatica[173].

Come si è esaminato, dunque, nell'ordinamento tedesco esistono diverse disposizioni che sanzionano gli atti preparatori alla commissione di reati contro il patrimonio. Va però evidenziato che analogamente a quanto avviene nell'ordinamento italiano, tutti questi reati preparatori sono tutti concepiti come reati minori, con sanzioni poco elevate. Questo potrebbe rappresentare un grosso limite, poiché, come si è esaminato sopra, ormai vi è un fiorente mercato di *hacker-tools* e coloro che effettivamente fanno uso di questi strumenti per commettere una frode informatica non sono le stesse persone che professionalmente si dedicano alla loro vendita. Sanzioni così lievi sono il retaggio di un'epoca storica in cui

[166] GALÁN MUÑOZ A., *Los ciberdelitos*, cit., p. 164.
[167] FARALDO CABANA P., *Las nuevas tecnologías*, cit., p. 113.
[168] SÁNCHEZ LINDE M., *Las Conductas del Artículo 248.2.B)*, cit., p. 385.
[169] FARALDO CABANA P., *Las nuevas tecnologías*, cit., p. 114.
[170] *Ibid*., p. 386.
[171] MIRÓ LLINARES F., *La respuesta penal al ciberfraude*, cit., p. 25.
[172] SÁNCHEZ LINDE M., *Las Conductas del Artículo 248.2.B)*, cit., p. 385.
[173] MIRÓ LLINARES F., *La respuesta penal al ciberfraude*, cit., p. 17.

l'*hacker* non era che un solitario esperto di informatica, ma rischiano di non essere idonee a consentire la repressione del complesso fenomeno criminoso *dell'hacking-as-a-service*, anche perché qualora il reato sia considerato bagatellare non sempre è possibile o comunque economicamente sostenibile l'attivazione degli strumenti europei di cooperazione giudiziaria.

Al contrario, nell'ordinamento spagnolo gli atti preparatori alla commissione dei reati contro il patrimonio sono puniti con la stessa pena delle ipotesi consumate di reati contro il patrimonio. Se da un lato le sanzioni elevate possono costituire un deterrente per il *cybercrime-as-a-service,* dall'altro lato vi può essere un problema di proporzionalità della pena.

3. La fase di interazione con i dati illecitamente carpiti.

3.1. L'accesso abusivo al sistema informatico.

Come sopra evidenziato, gli attacchi informatici contro il patrimonio si articolano di regola in più fasi, di cui l'ottenimento dell'ingiusto profitto costituisce solo l'ultima fase. È, dunque, opportuno esaminare quali fattispecie possono essere applicate alla seconda fase dei *phishing attacks*, ovvero di interazione coi dati illegittimamente carpiti.

Nell'ordinamento tedesco la tutela penale della riservatezza dei dati è affidata in via principale ai §§ 202a StGB relativo allo spionaggio di dati (*Ausspähen von Daten*)[174] e 202b StGB, che punisce l'intercettazione di dati (*Abfangen von Daten*), nonché al sopra esaminato § 202c StGB. Nell'ordinamento spagnolo, invece, l'accesso abusivo al sistema informatico e l'intercettazione dei dati sono sanzionate rispettivamente all'art. 197-*bis*.1 e 2 *código penal*, articolo introdotto dalla *Ley Orgánica* 1/2015 di recepimento della direttiva 2013/40/UE.

Il § 202a StGB fu introdotto nello *Strafgesetzbuch* già con la 2.WiKG cit., ma fu in seguito oggetto di parziali modifiche da parte della l. 11 agosto 2007 n. 1786 per sanzionare

[174] «*Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft. (2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden*» (Chiunque senza autorizzazione ottiene l'accesso non autorizzato, per sé o per altri, a dati che a lui non sono destinati e che sono particolarmente protetti contro l'accesso non autorizzato superando la sicurezza dell'accesso, è punito con la reclusione non superiore a tre anni o con una sanzione pecuniaria. (2) I dati ai sensi del comma (1) sono solo i dati che vengono memorizzati o trasmessi elettronicamente, magneticamente o in altro modo non direttamente percepibili).

le condotte di c.d. *hacking*[175]. A seguito di quest'ultima modifica, la precedente condotta di "procurarsi" i dati fu sostituita con quella odierna di "ottenere l'accesso non autorizzato ai dati"[176]. Inoltre, è stato specificato che l'accesso a tali dati deve avvenire "superando la protezione posta all'accesso"[177]. Si tratta di una disposizione posta a tutela del cd. domicilio informatico, ovvero della sfera della riservatezza informatica volta a proteggere i dati indipendentemente dal loro valore o contenuto[178]. L'Abs. 2 precisa poi che ai fini della legge penale i dati sono solo quelli elettronici, magnetici o altri non immediatamente percepibili, archiviati o trasmessi. La dottrina maggioritaria interpreta in senso lato tale concetto, ritenendo che consistano in caratteri o funzioni continue, che rappresentano informazioni sulla base di accordi noti o impliciti, indipendentemente dal fatto che siano a scopo di elaborazione, su codici binari o che siano dati personali[179]. La tutela, dunque, prescinde dal contenuto degli stessi dati. La norma precisa poi che i dati in questione non devono destinati al trasgressore. In merito a tale requisito, si evidenzia che non è rilevante la titolarità dei dati, quindi non occorre essere il gestore del sistema o il proprietario del supporto dei dati, ma è sufficiente che sia stata conferita la legittimazione all'accesso e a disporre dei dati stessi[180].

A differenza dell'art. 615-*ter* c.p. e, come si vedrà, dell'art. 197-*bis*.1 *código penal*, il §202a StGB non sanziona l'accesso in quanto tale, ma l'ottenimento dell'accesso ai dati contenuti nel sistema. A tal proposito, nella dottrina tedesca vi è chi ha evidenziato che la norma così formulata non sarebbe pienamente conforme agli *standard* richiesti dal legislatore europeo[181]. In effetti, l'art. 3 della direttiva 40/2013/UE cit. impone agli Stati membri di sanzionare «*l'accesso senza diritto a un sistema di informazione o a una parte dello stesso*», dunque il mero accesso al sistema, non ai dati in esso contenuti. È però anche vero che nella maggior parte dei casi colui che accede al sistema ottiene anche l'accesso ai dati in esso contenuti. Non si ritiene, invece, contraria agli obblighi previsti dalla menzionata direttiva la mancata punibilità del tentativo, dato che l'art. 8 co. 2 della stessa impone la punibilità del tentativo solo per i reati di interferenza illecita relativamente ai sistemi e ai dati. Per quanto riguarda il requisito della mancata autorizzazione (*Unbefugt*) si ritiene sia

[175] GRAF J.P., *sub StGB § 202a* in V. Erb, J. Schäfer (a cura di), *Münchener Kommentar zum Strafgesetzbuch*, VI ed. München, 2021, Rn. 1.
[176] GRÖSELING N., HÖFINGER F.M., *Hacking und Computerspionage*, cit., p. 550 ss.
[177] *Ibid*., p. 551.
[178] ERNST S., *Das neue Computerstrafrecht*, cit., p. 2661; p. 161.
[179] STUCKENBERG C.F., *Zur Strafbarkeit von "Phishing"*, cit., p. 883.
[180] MARBERTH-KUBICKI A., *Computer- und Internetstrafrecht*, cit., p. 44; GERCHE M., BRUNST P.W., *Praxishandbuch Internetstrafrecht*, cit., p. 67.
[181] SIEBER U., *sub § 24 Computerkriminalität*, in U. Sieber, H. Satzger, B. von Heintschel-Heinegg, *Europäisches Strafrecht*, Baden-Baden, 2014, p. 435 ss., p. 465; GRÖSELING N., HÖFINGER F.M., *Hacking und Computerspionage*, cit., p. 551.

clausola di antigiuridicità, che indica che il reo non dev'essere legittimato ad agire sui dati[182]. Essa però, esclude la tipicità del fatto nei casi in cui i dati in questione erano destinati alla conoscenza dell'autore dell'accesso[183]. A tal proposito va evidenziato che il § 202a StGB, a differenza dell'art. 615-*ter* c.p., non sanziona i casi in cui colui al quale è stato conferito il potere di accesso a tali dati, ma ne fa un utilizzo in contrasto con il contratto che regola l'accesso o con lo scopo per il quale l'accesso è stato conferito[184]. In ogni caso, si evidenzia che in quest'ultimo caso non è sufficiente la mera conoscenza della *password*, ma è necessario anche il conferimento del diritto di utilizzare i dati del programma in questione[185]. Ulteriore requisito è che l'accesso ai dati debba essere ottenuto superando la protezione dell'accesso. Tale requisito, che ha la funzione di escludere la punibilità dei casi meno gravi, richiede che per il superamento della protezione l'accesso richieda un tempo o uno sforzo tecnico non trascurabile[186]. Elemento soggettivo richiesto dalla norma è il dolo, che può essere anche eventuale[187].

L'applicazione *tout court* del § 202a StGB alla prima fase dei *phishing attacks* non è pacifica, perché è previsto che i dati in questione debbano essere protetti da "speciali misure di sicurezza" contro accessi abusivi (*gegen unberechtigten Zugang besonders gesichert sind*). La giurisprudenza interpreta rigorosamente tale requisito, richiedendo per l'applicazione del reato in questione che il programma di protezione sia adatto ad impedire l'accesso non autorizzato ai dati memorizzati e che non possa quindi essere superato senza conoscenze specialistiche[188]. Questo ne rende impossibile l'applicazione ai casi di *phishing*

---

[182] HILGENDORF E., VALERIUS B., *Computer- und Internetstrafrecht*, cit., p. 167.
[183] GRAF J.P., *sub StGB § 202a*, cit., Rn. 65.
[184] OLG Celle, ordinanza 31agosto 2016 - 2 Ss 93/16; EISELE J., *sub § 202a StGB*, in A. Schönke, H. Schröder (Hrsg), *Beck-Online Kommentar Strafgesetzbuch*, XXX ed., 2019, Rn. 12.
[185] KOCHHEIM D., *Cybercrime und Strafrecht*, cit., p. 241.
[186] WEIDEMANN M., *sub StGB § 202a*, in B. Von Heintschel-Heinegg (Hrsg), *Beck-Online Kommentar StGB*, cit., Rn. 19.
[187] *Ibid*., Rn. 21.
[188] «*Denn der Schutzbereich dieser Strafvorschrift erstreckt sich nur auf Daten, die gegen unberechtigten Zugang besonders gesichert sind. Dies sind nur solche, bei denen der Verfügungsberechtigte durch seine Sicherung sein Interesse an der Geheimhaltung der Daten dokumentiert hat. Die Zugangssicherung im Sinne von § 202 a Abs. 1 StGB muss darauf angelegt sein, den Zugriff Dritter auf die Daten auszuschließen oder wenigstens nicht unerheblich zu erschweren. Darunter fallen insbesondere Schutzprogramme, welche geeignet sind, unberechtigten Zugriff auf die auf einem Computer abgelegten Daten zu verhindern, und die nicht ohne fachspezifische Kenntnisse überwunden werden können und den Täter zu einer Zugangsart zwingt, die der Verfügungsberechtigte erkennbar verhindern wollte*» (L'ambito di protezione di questa disposizione penale si estende solo a dati particolarmente protetti contro l'accesso non autorizzato. Questi sono solo quelli in cui la persona autorizzata ha documentato il suo interesse per la riservatezza dei dati. La sicurezza di accesso ai sensi della sezione 202a (1) del codice penale deve essere concepita per escludere, o almeno rendere più gravoso, l'accesso di terzi ai dati. Ciò include in particolare programmi di protezione idonei per impedire l'accesso non autorizzato ai dati memorizzati su un computer e che non possono essere superati senza conoscenze specifiche e che costringono l'autore a un tipo di accesso che la vittima intendeva prevenire) così BGH, ordinanza 21.7.2015, 1 StR 16/15 in *NstZ*, 2016, p. 339 ss., p. 340.

semplice o classico, ove è la vittima stessa a fornire al reo i propri dati o le proprie credenziali[189]. Solo, quindi, in caso di successivo utilizzo delle credenziali d'accesso tramite l'utilizzo di codici PIN o *password* potrebbe configurarsi lo spionaggio di dati[190]. Nel caso del *phishing* classico, però si evidenzia che difetta anche il requisito della "non destinazione dei dati al trasgressore", poiché l'accesso a questi ultimi è stato volontariamente fornito dalla vittima. Qui vi è il consenso della vittima all'utilizzo dei dati, che rimane effettivo, anche se ottenuto con l'inganno e i dati vanno quindi qualificati come destinati all'autore del reato[191]. Non manca, tuttavia, chi ritiene anche in questo applicabile il §202a StGB, evidenziando che il consenso ottenuto con l'inganno non può essere ritenuto valido[192]. Tale reato trova, invece, applicazione laddove i dati relativi all'*account* di posta elettronica siano stati ottenuti utilizzando programmi informatici quali *trojan* o *keylogger* installati nel *computer* dell'utente, anche a seguito dell'invio di un'*e-mail* infetta, e che captano *password* e altri contenuti, perché in questo caso i dati vengono ottenuti tramite le modalità vietate dalla norma in questione, ovvero attraverso la violazione delle misure poste a protezione del sistema operativo e dei programmi[193]. Si esclude poi lo *skimming* dall'ambito di applicabilità della norma, poiché in questo caso non viene superata alcuna misura di protezione del sistema[194].

Reato analogo al §202a StGB previsto nell'ordinamento spagnolo è l'art. 197.*bis*.1 c.p., che sanziona colui che senza essere autorizzato e violando le misure di sicurezza acceda o fornisca l'accesso a tutto o parte di un sistema informativo a un'altra persona o si mantenga nello stesso contro la volontà della persona che ha il diritto legittimo di escluderlo[195]. Tale norma fu inizialmente introdotta nell'art. 197.3 *código penal* dalla *Ley Orgánica* 5/2010 cit. per sanzionare le condotte di *hacking*, che prima erano prive di specifica sanzione penale[196]

---

189 «*Nichts anderes gilt für die Fälle des Erschleichens von sonstigen Zugangsdaten, sodass jedenfalls der Phishing-Vorgang selbst nicht nach § 202a StGB strafbar ist*» (Non si applica altrimenti nei casi di altri dati d'accesso ottenuti con inganno, quindi in ogni caso il processo di phishing non è punibile secondo il § 202a StGB) così GRAF J.P., *"Phishing"*, cit., p. 131.

190 HANSEN D., *Strafbarkeit des Phishing*, cit., p. 164; STUCKENBERG C.F., *Zur Strafbarkeit von "Phishing"*, cit., p. 969.

191 EISELE J., *sub § 202a StGB*, in A. Schönke, H. Schröder (Hrsg), *Beck-Online Kommentar Strafgesetzbuch*, cit., Rn. 13. HANSEN D., *Strafbarkeit des Phishing*, cit., p. 164.

192 WEIDEMANN M., *sub StGB § 202a*, cit., Rn. 20.

193 GRAF J.P., *"Phishing"*, cit., p. 132.

194 WEIDEMANN M., *sub StGB § 202a*, cit., Rn. 18. In giurisprudenza v. BGH, Beschluss vom 06.07.2010 - 4 StR 555/09.

195 «*El que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años*».

196 SALVADORI I., *Los nuevos delitos informáticos*, cit., p.

e, a seguito della *Ley Orgánica* 1/2015, è finalmente divenuta fattispecie autonoma[197]. Prima della sua introduzione non si riteneva punibile la mera intrusione nel sistema informatico, la quale, però, poteva esserlo ai sensi dell'art. 197.1 c.p. (che verrà esaminato nel prosieguo), qualora l'accesso fosse stato finalizzato a svelare un segreto altrui[198]. Per altri ancora, l'accesso informatico poteva già essere punito a titolo di tentativo di violazione della *privacy* o di danneggiamento[199].

Controversa è l'individuazione del bene giuridico tutelato dall'197.*bis*.1 c.p. Vi è chi ritiene che esso non coincida con l'intimità della persona[200], ma che sia l'integrità e indennità del sistema informatico[201]. Per altri, invece, esso proteggerebbe il nuovo bene giuridico della riservatezza informatica[202]. La questione non è affatto priva di rilevanza pratica, perché l'art. 74.3 del *Código penal* impedisce l'applicazione dell'istituto del reato continuato in caso di offese a *bienes eminentemente personales*, come potrebbe essere l'intimità personale, mentre, in caso contrario, qualora si ritenga che la norma tuteli l'integrità del sistema informatico non vi sono problemi ad ammetterla[203].

Oggetto del reato è il sistema informatico, ovvero l'apparato o gruppo di apparati interconnessi o tra loro in relazione, che servono per realizzare il trattamento automatico dei dati informatici[204]. Le similitudini con l'art. 615-*ter* c.p. sono evidenti, perché anch'esso, al contrario del § 202a StGB, sanziona sia colui che accede al sistema senza autorizzazione, sia colui che si mantiene all'interno del sistema[205]. Si tratta, quindi, di condotte tra loro alternative[206], di cui la prima delle due sanziona i casi di mero *hacking*[207]. Dunque, analogamente all'art. 615-*ter* c.p., si sanziona il mero accesso, mentre non è necessario che sia stato arrecato alcun pregiudizio al titolare del sistema[208]. L'accesso può avvenire in qualsiasi modo o attraverso qualsiasi procedimento, sia agendo direttamente sul computer

[197] MORALES PRATS F., *La reforma de los delitos contra la intimidad*, cit., p. 465.
[198] MORÓN LERMA E., *Internet y Derecho Penal: Hacking y otras Conductas Ilícitas en la Red*, Cizur Menor, 2002, p. 60.
[199] GONZÁLEZ RUS J.J., *Daños a través de internet y denegación de servicios*, in Aa. Vv., *Homenaje al profesor Dr. Gonzalo Rodríguez Mourullo*, Navarra, 2005, p. 1469 ss., p. 1482.
[200] DEL VALLE SIERRA LÓPEZ M., *Los delitos de descubrimiento*, cit., p. 162.
[201] FERNÁNDEZ TERUELO J.G., *Derecho penal e internet*, cit., p. 197; DE LA MATA BARRANCO N. J., *Delitos contra los sistemas de información*, cit., p. 733.
[202] GALÁN MUÑOZ A., *Los ciberdelitos*, cit., p. 113.
[203] Cft. DE LA MATA BARRANCO N.J., *Delitos contra los sistemas de información*, cit., p. 735, il quale evidenzia che in caso di acceso abusivo a sistema informatico la giurisprudenza ritiene applicabile l'istituto del reato continuato, seppure sulla base di motivazioni diverse tra di loro.
[204] FERNÁNDEZ TERUELO J.G., *Derecho penal e internet*, cit., p. 201.
[205] SALVADORI I., *Los nuevos delitos informáticos*, cit., p. 231.
[206] DEL VALLE SIERRA LÓPEZ M., *Los delitos de descubrimiento*, cit., p. 162.
[207] SALVADORI I., *Los nuevos delitos informáticos*, cit., p. 232.
[208] FERNÁNDEZ TERUELO J.G., *Derecho penal e internet*, cit., p. 197.

sia attraverso l'utilizzo di programmi specifici quali *spyware*, *sniffers*, *keyloggers*, ecc.[209]. A differenza della fattispecie italiana, però, a seguito della riforma di cui alla *Ley Orgánica* 1/2015[210], si sanziona anche colui che agevoli l'accesso ad altri (*facilite a otro el acceso*). La condotta in questione è estranea al testo della direttiva 2013/40/UE, per cui si è trattato di una scelta del legislatore spagnolo. Trattasi, dunque, di qualificazione come *autoría* di un atto che in realtà sarebbe *participación*[211]. In quest'ultimo caso il terzo viene sanzionato indipendentemente dal fatto che colui che voleva aiutare riesca o meno ad accedere al sistema[212]. Per alcuni autori, però, con l'espressione "*facilitar el acceso*" non si intende la concessione della possibilità di fornire un qualsiasi tipo di aiuto o ausilio, ma solo della possibilità di accedere direttamente al sistema[213]. Altri ancora, invece, sostengono che per la punibilità di tale condotta è necessario che si verifichi un effettivo accesso al sistema informatico, poiché altrimenti vi sarebbe un inammissibile ampliamento delle condotte sanzionate e non sarebbe giustificata la comminazione della pena identica rispetto all'accesso[214]. Si evidenzia, però che questa soluzione non risolve il problema della sproporzione della pena, perché l'opera del complice, anche se minima, viene comunque equiparata a quella dell'autore che accede effettivamente al sistema[215].

L'accesso al sistema deve avvenire superando le misure di sicurezza poste a

---

[209] DE LA MATA BARRANCO N.J., *Delitos contra los sistemas de información*, cit., p. 734.
[210] MORALES PRATS F., *La reforma de los delitos contra la intimidad*, cit., p. 466.
[211] DEL VALLE SIERRA LÓPEZ M., *Los delitos de descubrimiento*, cit., p. 175. Nell'ordinamento spagnolo, infatti, analogamente all'ordinamento tedesco, non vige il principio di unità del concorso di persone del reato, ma si distingue tra *autoría* e *participación*. Gli autori vengono definiti dall'art. 28 del *código penal* come "*quienes realizan el hecho por sí solos, conjuntamente o por medio de otro del que se sirven como instrumento*". Nell'ambito della *autoría* si distingue tra autore diretto individuale, autore mediato, ovvero colui che realizza il fatto utilizzando un altro soggetto come mero strumento, e *coautoría*, ovvero la realizzazione congiunta di un delitto da parte di diverse persone che collaborano coscientemente e volontariamente. La *participación*, invece, è la cooperazione dolosa in un delitto doloso altrui ed è caratterizzata dal principio di accessorietà: la partecipazione dev'essere accessoria rispetto al fatto tipico e antigiuridico dell'autore. Nell'ambito della partecipazione si distingue tra l'istigazione e la cooperazione. In quest'ultimo caso, a sua volta, si distingue tra il cooperatore necessario e i complici. I primi ai sensi dell'art. 28 lett. b) c.p. vengono puniti come gli autori, mentre i complici ai sensi dell'art. 29 c.p. Generalmente la distinzione tra queste due figure viene individuata nella maggiore o minore importanza causale del contributo apportato. Per approfondire v. GÓRRIZ ROYO E., *El concepto de autor en derecho penal*, Valencia, 2008, p. 181 ss.; PEÑARANDA RAMOS E., *La participación en el delito y el principio de accesoriedad*, Madrid, 1990, p. 106 ss.; DÍAZ Y GARCÍA CONLLEDO M., *La autoría en Derecho penal*, Barcelona, 1991, p. 206 ss.; MIR PUIG S., *Derecho Penal. PG*, cit., p. 376 ss.; MUÑOZ CONDE F., GARCÍA ARÁN M., *Derecho Penal. PG*, cit., p. 408 ss.; In lingua inglese v. GARCÍA MAGNA D., *Principals and accessories*, in *Lessons of Spanish Substantive Criminal Law*, cit., p. 139 ss.
[212] GALÁN MUÑOZ A., *Los ciberdelitos*, cit., p. 119.
[213] *Ibid*., p. 120.
[214] COLÁS TURÉGANO A., *Nuevas conductas delictivas contra la intimidad (arts. 197; 197 bis; 197 ter)*, in J.L. González Cussac (dir.) e Á. Matallín Evangelio, E. Górriz Royo (coord.), *Comentarios a la Reforma del Código Penal de 2015*, Valencia, 2015, p. 663 ss., p. 676.
[215] GALÁN MUÑOZ A., *Los ciberdelitos*, cit., p. 120 s.

protezione del sistema, elemento che delimita l'ambito applicativo della fattispecie[216]. Neppure il legislatore spagnolo ha però definito che cosa debba intendersi per "*medidas de seguridad*", per cui esso viene interpretato in senso ampio, ricomprendendovi qualsiasi sistema specifico che renda visibile all'esterno la volontà di limitare l'accesso al sistema solo a determinate persone[217]. Il reato si consuma quando il reo riesce effettivamente ad accedere al sistema[218]. L'accesso, poi, non dev'essere stato autorizzato, dunque deve avvenire contro il consenso del titolare, requisito, questo, la cui sussistenza dovrà essere verificata nel singolo caso concreto[219].

Elemento soggettivo è il dolo generico[220], per cui non occorre che il reo agisca per un determinato fine. Anche per tale fattispecie trova applicazione la circostanza aggravante di cui all'art. 197-*quater* c.p. per il fatto commesso nell'ambito di un'organizzazione criminale.

Tale fattispecie può trovare durante la terza fase dei *phishing attacks*, quindi anche nel caso del *pharming*, dato che il reo accede al sistema informatico altrui modificando l'indirizzo IP o la configurazione DNS di un sistema informatico[221].

3.2. L'intercettazione di dati.

Per quanto riguarda l'intercettazione di dati, nell'ordinamento tedesco essa è punita dal § 202b StGB (*Abfangen von Daten*)[222], introdotto dalla già citata l. 11 agosto 2007 n. 1786 proprio per punire l'intercettazione delle *e-mail* e dei dati informatici, sia via cavo che *wireless*[223]. Bene giuridico tutelato da quest'ultima norma è identico a quello di cui al § 202a StGB, ovvero la riservatezza informatica[224]. Anche in questo caso oggetto del reato sono i

---

[216] *Ibid*., p. 118.
[217] FERNÁNDEZ TERUELO J.G., *Derecho penal e internet*, cit., p. 199; GALÁN MUÑOZ A., *Los ciberdelitos*, cit., p. 118; SALVADORI I., *Los nuevos delitos informáticos*, cit., p. 232.
[218] GALÁN MUÑOZ A., *Los ciberdelitos*, cit., p. 118.
[219] *Ibid.*, p. 116.
[220] DEL VALLE SIERRA LÓPEZ M., *Los delitos de descubrimiento*, cit., p. 163; FERNÁNDEZ TERUELO J.G., *Derecho penal e internet*, cit., p. 202.
[221] FLOREZ MENDOZA M., *Respuesta penal al denominado robo de identidad*, cit., p. 318.
[222] «*Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§ 202a Abs. 2) aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist*» (Chiunque utilizzando mezzi tecnici ottenga senza autorizzazione per sè o per altri dati a lui non destinati, da una trasmissione di dati non pubblica o dalle onde elettromagnetiche di un sistema di elaborazione dati, è punito con la pena detentiva non superiore a due anni o con la pena pecuniaria, se il fatto non costituisce più grave reato).
[223] ERNST S., *Das neue Computerstrafrecht*, cit., p. 2662.
[224] WEIDEMANN M., *sub StGB § 202b*, in B. Von Heintschel-Heinegg (Hrsg), *Beck-Online Kommentar StGB*, cit., Rn. 2.

dati, anch' essi "non destinati al trasgressore", ma solo quelli in corso di trasmissione al momento del reato[225]. Tali dati, inoltre, devono provenire da una trasmissione di dati non pubblica o dalle onde elettromagnetiche di un sistema di elaborazione dati. Per trasmissione di dati si intende qualsiasi forma concepibile di trasmissione degli stessi, quali ad esempio le trasmissioni nell'ambito di connessioni *wireless* (*WLAN*), le trasmissioni via *e-mail*, telefono, *modem*, *voice over IP*, fax, ecc.[226]. Dunque, in conformità con l'art. 3 della Convenzione *cybercrime*, il processo di trasmissione non è limitato ad *Internet*, ma comprende anche quello che può avvenire all'interno dello stesso sistema informatico. In ogni caso, si tratta però di un trasferimento di dati immateriali[227].

A differenza del § 202a StGB, nel § 202b è necessario che i dati siano effettivamente ottenuti, non è sufficiente riuscire ad avere ad essi accesso[228]. Inoltre, è richiesto che la trasmissione dei dati sia "non pubblica": a tal scopo non rileva il tipo o il contenuto dei dati trasmessi, ma si deve fare riferimento al § 201 Abs. 2 Nr. 2 StGB[229]. In definitiva, si tratta soprattutto di stabilire se il trasferimento dei dati è diretto e destinato a un gruppo più ampio di persone indeterminate in termini di numero e individualità o non collegate tra loro da rapporti personali o materiali. A tal fine, decisiva è la determinazione concreta da parte del titolare del trattamento è decisiva[230]. Se la trasmissione di dati è liberamente disponibile su Internet, non è protetta dalla sezione 202b, né lo è se è diretta a un gruppo indeterminato di destinatari[231].

La condotta sanzionata consiste nell'ottenimento dei dati con mezzi tecnici. Ottenere significa avere il controllo effettivo dei dati, il che può avvenire copiandoli su un supporto, annotandoli o registrandoli in qualsiasi altro modo, mentre nel caso delle *e-mail* è sufficiente la loro lettura, Se, invece, i dati sono criptati, possono considerarsi "ottenuti" solo quando la crittografia è stata violata o la chiave sottostante è stata ottenuta con successo[232]. Per mezzi tecnici, invece, si intendono sia mezzi *hardware*, sia i dispositivi di comunicazione *wireless*,

---

[225] SCHUMANN K.H., *Das 41. StrÄndG zur Bekämpfung der Computerkriminalität*, in *NStZ*, 2007, p. 675 ss., p. 677; HILGENDORF E., VALERIUS B., *Computer- und Internetstrafrecht*, cit., p. 169.
[226] GERCHE M., BRUNST P.W., *Praxishandbuch Internetstrafrecht*, cit., p. 71 s.; HILGENDORF E., VALERIUS B., *Computer- und Internetstrafrecht*, cit., p. 170; WEIDEMANN M., *sub StGB § 202b*, cit., Rn. 5.
[227] GRÖSELING N., HÖFINGER F.M., *Hacking und Computerspionage*, cit., p. 552.
[228] MARBERTH-KUBICKI A., *Computer- und Internetstrafrecht*, cit., p. 59.
[229] GRAF J.P., *sub StGB § 202b*, in V. Erb, J. Schäfer (a cura di), *Münchener Kommentar zum Strafgesetzbuch*, VI ed. München, 2021, Rn. 10.
[230] *Ibid*.
[231] GERCHE M., BRUNST P.W., *Praxishandbuch Internetstrafrecht*, cit., p. 71.
[232] GRAF J.P., *sub StGB § 202b*, cit., Rn. 16.

software, codici o *password*[233]. Infine, anche in questo caso elemento soggettivo è il dolo, che può essere anche eventuale[234].

Nell'ambito applicativo della norma in questione rientrano senz'altro gli attacchi di *phishing* "*man-in-the-middle*", ove il *phisher* intercetta i messaggi indirizzati ad un sito scelto da un utente indeterminato, salva le informazioni che gli interessano, poi trasmette i messaggi al sito scelto dalla vittima e poi inoltra le risposte di ritorno[235]. Non vi rientrano, invece, i casi di *phishing* classico, in quanto in quest'ultimo caso i dati non vengono intercettati[236]. La norma, inoltre, sanziona l'uso di *virus* di tipo *trojan* quali *sniffer* o *keylogger*, che consentono ai criminali informatici di registrare il traffico di dati o i tasti premuti dalla vittima[237]. Se l'autore del reato si è procurato dapprima i dati per poi trasmetterli, la trasmissione dei dati costituisce un diverso reato rispetto al precedente ottenimento dei dati[238].

Nell'ordinamento spagnolo, invece, l'intercettazione di dati è punita dall'art. 197-*bis*.2 c.p.[239], comma introdotto *ex novo* dalla *Ley Orgánica* 1/2015 cit. e che ricalca la formulazione dell'art. 6 della direttiva 2013/40/UE. Alcuni autori hanno criticato l'introduzione di questa nuova fattispecie, evidenziando che la stessa sanziona l'intercettazione non pubblica di dati, condotta identica a quella già sanzionata dall'art. 197.1 c.p. già in vigore (che, come si esaminerà nel prosieguo, sanziona proprio l'intercettazione di telecomunicazioni), tuttavia punita con una pena sensibilmente inferiore[240]. Si evidenzia però che nell'introdurre tale norma lo stesso legislatore, nel preambolo della *Ley Orgánica*, ha specificato che mentre il 197.1 c.p. sanziona l'intercettazione di comunicazioni che avvengono tra persone attraverso *chat*, *mail*, *whatsapp*, ecc., la norma in questione punisce l'intercettazione di comunicazioni automatizzate che avvengono tra sistemi, ovvero la trasmissione di dati, per cui è in ciò che consiste la differenza tra i due reati[241]. L'art. 197 *bis*.2 c.p. precisa che le trasmissioni in questione non devono essere pubbliche, requisito che secondo il preambolo alla *Ley Orgánica* 1/2015, indica che oggetto della norma debbono

[233] GERCHE M., BRUNST P.W., *Praxishandbuch Internetstrafrecht*, cit., p. 73.
[234] SCHUMANN K.H., *Das 41. StrÄndG*, cit., p. 677.
[235] WEIDEMANN M., *sub StGB § 202b*, cit., Rn. 9.
[236] *Ibid*.
[237] HILGENDORF E., VALERIUS B., *Computer- und Internetstrafrecht*, cit., p. 169.
[238] GRAF J.P., *sub StGB § 202b*, cit., Rn. 17.
[239] «*El que mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos, será castigado con una pena de prisión de tres meses a dos años o multa de tres a doce meses*».
[240] MORALES PRATS F., *La reforma de los delitos contra la intimidad*, cit., p. 466.
[241] GALÁN MUÑOZ A., *Los ciberdelitos*, cit., p. 124.

essere "trasmissioni tra sistemi, che non siano personali"[242]. Si ritiene, dunque, che la norma in questione si riferisca alle trasmissioni che avvengono tra i sistemi informatici in forma automatizzata, quali ad esempio i dati che il singolo dispositivo invia al ripetitore per la connessione alla rete[243].

La condotta sanzionata consiste nell'intercettare dati utilizzando artifici o strumenti tecnici, ovvero meccanismi o programmi atti a consentire l'intercettazione[244]. Anche in questo caso, analogamente all'art. 197 *bis*.1 c.p., occorre che il reo agisca "senza essere stato debitamente autorizzato", requisito che va interpretato alla luce dell'art. 2 lett. d) della direttiva 2013/40/UE, per cui si ritiene debba mancare il consenso di colui che ne possa disporre e che l'intercettazione debba avvenire al di fuori dei casi consentiti dalla legge[245]. Analogamente all'art. 617-*quater* del codice penale italiano e al § 202b StGB, elemento soggettivo è il dolo generico, per cui non occorre che il reo agisca per un fine particolare[246].

Nell'ambito applicativo della norma in questione, dunque, rientra l'utilizzo di tutte quelle *app* di *keylogger* che, utilizzando le onde radio emesse dal *monitor* o da un *display* collegato ad un computer, permettono di intercettare tutto quel che si digita su un computer a poca distanza[247]. Anche in quest'ultimo caso si applica la circostanza aggravante di cui all'art. 197-*quater* c.p. per il fatto commesso nell'ambito di un'organizzazione criminale.

3.3. La ricettazione di dati

Va poi evidenziato che, a differenza che in Italia e Spagna, in Germania esiste, oltre al già menzionato § 202c, un'altra fattispecie applicabile alla seconda fase dei *phishing attacks*, ovvero la ricettazione di dati (*Datenhehlerei*) di cui al § 202d StGB[248]. Nell'ordinamento spagnolo all'art. 197.3 c.p. è però presente un'ipotesi delittuosa aggravata per il caso di diffusione, divulgazione o trasmissione di dati personali ottenuti mediante le modalità illecite descritte dall'art. 197.1 e 2 c.p.[249].

---

[242] Cft. il *Preámbulo* alla *Ley Orgánica* 1/2015, disponibile *online* al sito https://www.boe.es.
[243] GALÁN MUÑOZ A., *Los ciberdelitos*, cit., p. 124.
[244] COLÁS TURÉGANO A., *Nuevas conductas delictivas contra la intimidad*, cit., p. 679.
[245] GALÁN MUÑOZ A., *Los ciberdelitos*, cit., p. 126.
[246] *Ibid*.
[247] DE LA MATA BARRANCO N. J., *Delitos contra los sistemas de información*, cit., p. 736.
[248] «*Wer Daten, die nicht allgemein zugänglich sind und die ein anderer durch eine rechtswidrige Tat erlangt hat, sich oder einem anderen verschafft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, um sich oder einen Dritten zu bereichern oder einen anderen zu schädigen, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft*» (Chiunque ottiene, fornisce, consegna, distribuisce o comunque rende disponibili dati che non sono generalmente accessibili e che sono stati ottenuti da un'altra persona con un atto illecito, al fine di arricchire se stesso o un terzo o di danneggiare un'altra persona, è punito con la reclusione fino a tre anni o con la multa).
[249] GALÁN MUÑOZ A., *Los ciberdelitos*, cit., p. 86.

Il § 202d StGB è stato introdotto nello *Strafgesetzbuch* dalla legge del 10 dicembre 2015 sull'introduzione di un obbligo di conservazione e di un periodo massimo di conservazione dei dati sul traffico (*Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten beschlossen*). Il suo inserimento nello *Strafgesetzbuch* è dovuto alla necessità di colmare un vuoto normativo, perché la compravendita di dati illecitamente carpiti non poteva essere sanzionata ai sensi del § 259 StGB, che punisce la ricettazione (*Hehlerei*), non potendo i dati essere considerati "cose" (*Sachen*)[250]. Il nuovo reato punisce chiunque ottiene, fornisce, consegna, distribuisce o mette altrimenti a disposizione di un'altra persona i dati definiti dal § 202a par. 2, che non sono generalmente accessibili e che un'altra persona ha ottenuto con un atto illecito. È evidente, quindi, la similitudine con il reato tradizionale di ricettazione, dato che in entrambi i casi l'oggetto del reato deve provenire da un reato presupposto, che può essere anche la stessa ricettazione di dati[251]. Con riguardo alle condotte sanzionate, l'ottenimento dei dati per sé o per altri significa ottenere l'effettivo potere di disporre di tali dati, sia copiandoli su un proprio supporto di memorizzazione, sia registrandoli in qualsiasi altra maniera[252]. L'attenzione posta dal legislatore con riferimento all'ottenimento del potere effettivo di disporre dei dati solleva qualche perplessità in dottrina, perché pur avendosi ricettazione di dati, i dati originali rimangono a disposizione dell'avente diritto, a meno che non vengano eccezionalmente cancellati o resi inutilizzabili[253]. La seconda condotta sanzionata consiste nella fornitura, ovvero nel trasferimento dei dati ad un'altra persona[254]. La diffusione, invece, consiste nella trasmissione di dati con l'obiettivo di rendere i dati accessibili a una cerchia più ampia di utenti. Infine, la messa a disposizione consiste nel dare la possibilità di accedere ai dati, ovvero la possibilità di "scaricarli" da un supporto di memorizzazione o comunque di accedervi elettronicamente[255]. Nonostante la rubrica, è evidente l'analogia con l'art. 615-*quater* c.p. del codice penale italiano, dato che le condotte sanzionate dal §202d StGB corrispondono ad alcune di quelle sanzionate dalla disposizione italiana. Inoltre, anche la fattispecie tedesca richiede il dolo specifico, poiché il fatto dev'essere commesso allo scopo di arricchire se stessi o un terzo o di nuocere ad un altro[256]. Tale norma, dunque, diverge

[250] GRAF J.P., *sub § 202 d StGB*, in *Münchener Kommentar zum StGB*, III ed., 2017, par. I.
[251] GERCHE M., *Die Entwicklung des Internetstrafrechts 2015/2016*, in *ZUM*, 2016, p. 825 ss., p. 828
[252] GRAF J.P., *sub § 202 d StGB*, cit., par. I sez. 2
[253] EISELE J., *sub § 202 d StGB, cit.*, par. I
[254] GRAF J.P., sub § 202 d StGB, cit., par. I sez. 2
[255] *Ibid*.
[256] EISELE J., *sub § 202 d StGB*, in A. Schönke, H. Schröder (Hrsg), *Beck-Online Kommentar Strafgesetzbuch*, cit., Rn. 2. Va precisato che il codice penale tedesco non contiene una definizione generale di delitto doloso, ma si usa distinguere tre forme del dolo: dolo intenzionale (*Absicht o dolus directus ersten Grades*), dolo diretto

dall'art. 615-*quater* c.p. per quanto riguarda l'oggetto del reato, che in quest'ultimo caso è più ampio, perché la fattispecie tedesca si limita a menzionare i dati, non richiedendo che gli stessi siano idonei all'accesso ad un sistema informatico.

Ulteriore requisito della fattispecie tedesca è la non accessibilità dei dati (*die nicht allgemein zugänglich sind*): il § 10 co. 5 della *Bundesdatenschutzgesetz* contiene una definizione legale del termine "generalmente accessibile", che viene utilizzato anche nel § 202d StGB. Ai sensi di tale norma i dati sono "generalmente accessibili" quando chiunque può utilizzarli, senza o dopo la previa registrazione, l'approvazione o il pagamento di una tassa[257]. La dottrina ha criticato l'introduzione di questo requisito, evidenziando che lo stesso finisce per limitare notevolmente il campo applicativo della fattispecie[258]. È, infatti, controverso se i dati disponibili sul *dark web* possano o meno essere considerati "generalmente accessibili". Una parte della dottrina propende per la soluzione negativa, evidenziando che in linea di principio i dati caricati sul *dark web* sono utilizzabili da tutti perché in tale spazio virtuale normalmente non è richiesta alcuna registrazione o approvazione, per cui sono quindi generalmente accessibili[259]. Altri autori evidenziano che ciò che conta è che i dati non siano accessibili al pubblico e che anche se l'accesso sul *dark web* è tecnicamente facile, ciò non significa che le informazioni ricercate siano facili da trovare, perché senza indicizzazione da parte di un motore di ricerca, senza accesso a liste di indirizzi affidabili, senza invito a un gruppo, gran parte dei dati non è generalmente accessibile[260]. In particolare, vi è chi evidenzia che dati personali altrui quali numeri e codici di carte di credito, credenziali, ecc. non vengono semplicemente pubblicati sul *dark web*, ma vengono resi disponibili soltanto all'acquirente, il quale è l'unico che può prenderne cognizione, e solo a seguito del buon fine della transazione[261]. A supporto di tale tesi si fa presente che la stessa *Bundesverfassungsgericht* tedesca definisce come "fonte di informazione generalmente accessibile" solo quella tecnicamente idonea e destinata a fornire

(*direkten Vorsatz o dolus direcuts zweiten Grades*) e dolo eventuale (*bedingte Vorsatz*), mentre non si rinviene una nozione corrispondente al dolo specifico italiano. Il dolo intenzionale sussiste allorché un determinato scopo (*Absicht*) sia il movente principale della condotta. Nell'ordinamento tedesco, dunque, l'*Absicht* viene qualificata solo sul piano psicologico, in quanto immediata direzione della volontà alla realizzazione dell'evento, mentre non è richiesta la sua effettiva realizzazione per la consumazione del reato. Sul dolo nell'ordinamento tedesco v. per tutti PICOTTI L., *Il dolo specifico*, cit., p. 334 ss.

[257] «*Allgemein zugänglich sind Daten, die jedermann, sei es ohne oder nach vorheriger Anmeldung, Zulassung oder Entrichtung eines Entgelts, nutzen kann*».

[258] GERCHE M., *Die Entwicklung des Internetstrafrechts*, cit., p. 828

[259] STAM F., *Die Datenhehlerei nach § 202d StGB - Anmerkungen zu einem sinnlosen Straftatbestand*, in *StV*, 2017, p. 488 ss., p. 489; GERCHE M., *Die Entwicklung des Internetstrafrechts 2015/2016*, cit., p. 829.

[260] v. HENSLER S., *Datenhehlerei (§ 202 d StGB) bei Rückerlangung von Kundendaten*, in *NStZ*, 2020, p. 258 ss., p. 261.

[261] WEBER A., *Die Strafbarkeit von Plattformbetreibern*, cit., p. 212.

informazioni al grande pubblico, ovvero a persone non previamente individuate[262]. Inoltre, si sottolinea che l'obiettivo perseguito dal legislatore con l'introduzione di tale norma è proprio quello di punire il commercio di dati ottenuti mediante spionaggio o intercettazione, dati che in origine erano riservati o comunque "non generalmente accessibili" e, dunque, non appare corretto perdano questa loro caratteristica intrinseca solo perché un terzo li ha resi generalmente accessibili attraverso un atto illegale[263]. Questa appare essere l'interpretazione preferibile, poiché più coerente con la *ratio* della sua introduzione. Infatti, seguendo l'interpretazione contraria si renderebbe la fattispecie inapplicabile proprio ai casi che si volevano sanzionare. Infatti, solo così è possibile ritenere che la norma sia idonea a sanzionare fenomeni quale il *carding* e il fenomeno del *phishing-as-a-service*, ove, come si è esaminato, le compravendite avvengono quasi esclusivamente sul *dark web*. Tuttavia, va evidenziato che analogamente a quanto avviene nell'ordinamento italiano nel reato di ricettazione di cui all'art. 648 c.p., l'autore del reato presupposto non può essere punito ai sensi del § 202d StGB[264]. Dunque, poiché nella quasi totalità dei casi è colui che si procura tali dati a metterli in vendita, condotta che è già sanzionata dal § 202c StGB, troverà applicazione solo quest'ultima fattispecie, punita meno gravemente. Pertanto, neppure il § 202d StGB sembra essere pienamente idoneo a sanzionare la seconda fase dei *phishing attacks* o in generale il fenomeno del *Cybercrime-as-a-service*.

3.4. Le fattispecie a tutela dei dati personali

Durante la fase della c.d. interazione coi dati illecitamente carpiti viene in rilievo anche la tutela dei dati personali. Nell'ordinamento tedesco altra norma rilevante che può trovare applicazione è il § 42 della nuova *Bundesdatenschutzgesetz* (BDSG-neu)[265], ovvero la legge federale tedesca di protezione dei dati personali, entrata in vigore il 25 maggio 2018,

[262] BVerfGE 27, sentenza 3 ottobre 1969 - 1 BvR 46/65.
[263] *Ibid*.
[264] GERCHE M., *Die Entwicklung des Internetstrafrechts 2015/2016*, cit., p. 829.
[265] «*(1) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer wissentlich nicht allgemein zugängliche personenbezogene Daten einer großen Zahl von Personen, ohne hierzu berechtigt zu sein, 1.einem Dritten übermittelt oder 2.auf andere Art und Weise zugänglich macht und hierbei gewerbsmäßig handelt. (2) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer personenbezogene Daten, die nicht allgemein zugänglich sind, 1.ohne hierzu berechtigt zu sein, verarbeitet oder 2.durch unrichtige Angaben erschleicht und hierbei gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen*» ((1) Chiunque, agendo a titolo professionale, fornisce consapevolmente i dati personali di un gran numero di persone che non sono generalmente accessibili senza averne diritto, 1.trasmettendoli a terzi o 2. rendendoli accessibili in qualsiasi altro modo persona è punito con la reclusione fino a tre anni o con la multa. (2) Chiunque, agendo a scopo di lucro o con l'intenzione di arricchirsi o di danneggiare un'altra persona, fornisce dati personali non accessibili a tutti, 1. senza esserne autorizzato, trattati o 2. ottenuti con mezzi fraudolenti è punito con la reclusione fino a due anni o con la multa).

che ha sostituito la vecchia *Bundesdatenschutzgesetz* del 1 gennaio 1978. Tale articolo, introdotto dalla nuova legge sull'adeguamento e l'attuazione della protezione dei dati personali del 20 giugno 2017 (*Bundesdatenschutzgesetz vom 30. Juni 2017*), novella di adeguamento al Regolamento 2016/679/UE o GDPR e di attuazione della direttiva 2016/680/UE[266], prevede al par. 1 una nuova fattispecie che punisce la fornitura abusiva di dati personali di soggetti terzi da parte di un operatore professionale, mentre al par. 2 riprende la vecchia fattispecie di cui all'abrogato § 44 BDSG, sanzionando la fornitura abusiva di dati personali altrui non generalmente accessibili per fini illeciti.

La fattispecie in esame può trovare applicazione nella seconda fase dei *phishing attacks* proprio perché, a differenza di quella parallela italiana, è posta a tutela di tutte le categorie di dati personali, non solo di alcune[267], dunque anche di *password*, dati relativi ai pagamenti e alle carte di credito, agli indirizzi IP e a qualsiasi informazione concernente una persona fisica identificata o identificabile[268]. Non solo, ma si è evidenziato che anche se nel *phishing* classico è la stessa vittima a fornire i dati al reo, il consenso in merito al trattamento dei dati non è comunque sussistente ai sensi della disciplina sul trattamento dei dati personali, per cui tale condotta rientra senz'altro tra quelle sanzionate dalla norma in questione[269].

Per quanto riguarda il rapporto tra le norme, tra tale ultima fattispecie esaminata e i reati di cui ai §§ 202a e ss. StGB e i reati di falso di cui ai §§ 267 ss. StGB si configura l'unità d'azione (*Tateinheit*)[270] per cui, ai sensi del § 52 StGB, deve trovare applicazione il solo reato più grave[271]. Il reato di cui al § 42 Abs. 2 BDSG-neu è del resto sussidiario rispetto al § 42 Abs. 1 BDSG-neu[272].

---

[266] Direttiva relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati.

[267] EHMANN E., *BDSG § 42 Strafvorschriften*, in P. Gola, D. Heckman, *Bundesdatenschutzgesetz*, XIII ed., 2019, München, par. 7.

[268] BRODOWSKY D., NOWAK D., *BDSG § 42 Strafvorschriften*, in H. A. Wolff, S. Brink (Hrsg.), *BeckOK Datenschutzrecht*, XXX ed., München, 2020, par. 22.

[269] HANSEN D., *Strafbarkeit des Phishing*, cit., p. 119 ss.

[270] Il codice penale tedesco ai §§ 52 e 53 disciplina rispettivamente il concorso ideale/fatto unico (*Tateinheit*) e il concorso reale/fatto plurimo (*Tatmehrheit*). Si ha concorso ideale di reati allorché l'autore con la stessa condotta violi più disposizioni penali o più volte la stessa disposizione penale. Si ha, invece, concorso reale di reati qualora l'autore abbia commesso più fatti autonomi di reato che vengono tra loro giudicati nello stesso processo. Nel primo caso il fatto viene considerato come unico e punito con la sola pena prevista per il reato più grave, mentre nel secondo caso vi è concorso di reati, con applicazione di una pena cumulativa. In tale contesto, l'unità di azione è un presupposto del fatto unico punito secondo le regole del concorso ideale, mentre la pluralità di azioni a sua volta è un presupposto del fatto plurimo. Per approfondire v. PUPPE I., *Was ist Gesetzeskonkurrenz?*, in *JuS*, 2016, p. 961 ss.; ROXIN C., *Strafrecht Allgemeiner Teil*, vol. II, München, 2003, p. 833 ss.

[271] BRODOWSKY D., NOWAK D., *BDSG § 42 Strafvorschriften*, par. 67.

[272] *Ibidem*.

Anche nel codice penale spagnolo sono presenti disposizioni a tutela del bene giuridico dell'intimità informatica e dei dati personali[273]. Si tratta, in particolare, dei due commi dell'Art. 197.1 e 2 *Código penal*. L'art. 197.1 sanziona la scoperta e la rivelazione di segreti[274]. Bene giuridico protetto dalla norma è l'intimità personale[275], anche se vi è chi ritiene che sia anche «*la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos*»[276]. Le condotte sanzionate sono tre, ovvero l'impossessamento di documenti, le lettere, i messaggi di posta elettronica o qualsiasi altro documento o effetto personale di un'altra persona, l'intercettazione delle comunicazioni e l'utilizzo di strumenti tecnici di ascolto, trasmissione, registrazione, o riproduzione del suono o dell'immagine o di qualsivoglia altro segnale di comunicazione[277]. Anche in questo caso trattasi di norma a più fattispecie, nella quale le condotte sono tra loro alternative[278]. In ogni caso, per la consumazione del reato non occorre che l'autore riesca effettivamente nel suo intento[279]. Trattasi, dunque, di reato di pericolo[280]. Per quanto riguarda l'impossessamento, alcuni autori ritengono debba necessariamente consistere nell'apprensione di un oggetto materiale[281]. Altri, invece, dato che la stessa norma fa riferimento alle *e-mail*, ritengono che tale condotta possa consistere anche nella captazione di *e-mail* o SMS, dunque oggetti immateriali[282]. Con riferimento, invece, alle comunicazioni, si ritiene che in tale nozione siano ricomprese le piattaforme di messaggistica quali ad es. *Whatsapp*, dato che le stesse non sono espressamente menzionate con riguardo all'impossessamento[283]. Per tutte e tre le

[273] MATA Y MARTÍN R.M., *Delincuencia informática y derecho penal*, Madrid, 2001, p. 125.
[274] «*El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses*».
[275] GALÁN MUÑOZ A., *Los ciberdelitos*, cit., p. 71; MATA Y MARTÍN R.M., *Delincuencia informática*, cit., p. 125
[276] RUEDA MARTÍN A.M., *La confidencialidad, integridad y disponibilidad de los sistemas de información como bien jurídico protegido en los delitos contra los sistemas de información en el código penal español*, in *Riv. trim. Dir. pen. cont.*, 2020, n. 3, p. 199 ss., p. 206.
[277] MUÑOZ CONDE F., *Derecho Penal*, cit., p. 293 s.
[278] GALÁN MUÑOZ A., *Los ciberdelitos*, cit., p. 57.
[279] Tribunal Supremo, sez. I penale, sentenza 30 aprile 2007, n. 358.
[280] MATA Y MARTÍN R.M., *Delincuencia informática*, cit., p. 129.
[281] MUÑOZ CONDE F., *Derecho Penal. PE* , cit., p. 293; MATA Y MARTÍN R.M., *Delincuencia informática*, cit., p. 128; FLORES PRADA I., *Criminalidad informática*, cit., p. 63; MORALES PRATS F., *Del descubrimiento y revelación de secretos*, in G. Quintero Olivares (dir.), F. Morales Prats (coord.), *Comentarios a la parte especial del derecho penal*, cit., p. 436 ss., p. 439 evidenzia che l'intercettazione, riproduzione o registrazione illecita di un messaggio elettronico rientra già nell'intercettazione sanzionata dalla medesima norma, per cui l'impossessamento dev'essere limitato unicamente ai messaggi già stampati.
[282] GALÁN MUÑOZ A., *Los ciberdelitos*, cit., p. 58; FERNÁNDEZ TERUELO J.G., *Derecho penal e internet*, cit., p. 128; ANARTE BORRALLO E., *Consideraciones sobre los delitos de descurimiento de secretos (I). En especial, el artículo 197.1. del Código penal*, in 2002, 43, p. 50 ss., p. 54.
[283] GALÁN MUÑOZ A., *Los ciberdelitos*, cit., p. 60.

ipotesi è prevista la clausola di antigiuridicità speciale, perché la norma richiede che le condotte siano compiute senza il consenso del titolare del segreto[284]. Per quanto riguarda l'elemento soggettivo, trattasi di dolo specifico, poiché si richiede che l'agente agisca al fine di scoprire i segreti altrui o comunque turbarne l'intimità[285]. Alcuni autori, dunque, escludono sia possibile sanzionare le condotte descritte nella norma a titolo di dolo eventuale[286].

Con riferimento alla nozione di segreto, non rileva la sua natura pubblica o privata, non essendovi alcuna specificazione nella norma[287]. Vi è, dunque, chi ritiene che le credenziali di accesso al sistema informatico per lo svolgimento di operazioni bancarie possano considerarsi informazioni personali o private, per cui anche il *phishing* in senso lato potrebbe rientrare nell'ambito applicativo della norma in questione[288]. Non manca però chi dubita che questo sia corretto, evidenziando che il *Tribunal Supremo* ha specificato che oggetto del reato di cui all'art. 197.1 c.p. non è qualsiasi segreto, ma solo quello relazionato con l'intimità personale[289]. Con riferimento al concetto di "intimità personale", il *Tribunal Constitucional* ha affermato che esso ricomprende anche dati personali patrimoniali "se relativi all'intimità personale"[290]. Tuttavia, nel caso del *phishing*, i dati non sono che mere credenziali bancarie, le quali difficilmente contengono in sé informazioni personali, che invece contiene ad esempio un estratto conto bancario[291]. Per cui la mera apprensione di *password* o dati di carte di credito mediante uno *sniffer* non rientrerebbe nell'ambito applicativo della norma in questione, la quale, invece, può sanzionare i casi di *phishing* in cui vi è l'intercettazione massiccia di *e-mail*, credenziali e file di questo tipo, dato che in questo caso sussisterebbe la volontà di scoprire un segreto[292].

L'art. 197.2 c.p., invece, sanziona l'abuso di dati di carattere personale[293]. Tale

---

[284] *Ibid*., p. 63.
[285] MUÑOZ CONDE F., *Derecho Penal. PE*, cit., p. 294; FERNÁNDEZ TERUELO J.G., *Derecho penal e internet*, cit., p. 187.
[286] GALÁN MUÑOZ A., *Los ciberdelitos*, cit., p. 66.
[287] MUÑOZ CONDE F., *Derecho Penal. PE*, cit., p. 293. MORALES PRATS F., *Del descubrimiento y revelación de secretos*, cit., p. 441 critica l'utilizzo del termine "segreto", evidenziando che lo stesso è in realtà un contenitore vuoto che può avere ad oggetto una molteplicità di interessi e beni giuridici, per cui sarebbe stato più opportuno mantenere unicamente la locuzione "ledere l'intimità altrui".
[288] FLOREZ MENDOZA M., *Respuesta penal al denominado robo de identidad*, cit., p. 315; AGUADO LÓPEZ S., ORTIZ NAVARRO J.F., CABEDO VILLAMÓN F., *Istrucción y enjuiciamiento*, cit., p. 107.
[289] MATA Y MARTÍN R.M., *Delincuencia informática*, cit., p. 125.
[290] Tribunal Constitucional, sez. II, sentenza 26 settembre 2005, n. 233.
[291] MIRÓ LLINARES F., *La respuesta penal al ciberfraude. Especial atención a la responsabilidad de los muleros del phishing*, in *RECPC*, n. 15-12, p. 12:1 ss, p. 21.
[292] *Ibid*., p. 22.
[293] «*Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o*

disposizione è formata da due incisi: il primo sanziona colui che senza autorizzazione si impossessi, utilizzi o modifichi, a danno di terzi, dati personali o familiari riservati di un'altra persona, mentre il secondo colui che, senza esserne autorizzato, acceda a tali dati con qualsiasi mezzo, li alteri o li utilizzi a danno del titolare dei dati o di un terzo[294]. Vi è chi evidenzia che in realtà non vi è differenza tra i due incisi, che sono praticamente identici, dato che l'unica differenza riguarda il soggetto passivo[295]. L'individuazione del bene giuridico tutelato dalla norma in questione risulta estremamente controversa: per alcuni è l'intimità[296], per altri sono i dati personali[297]. Per la giurisprudenza del *Tribunal Supremo*, invece, è la libertà di informazione intesa come diritto del cittadino a controllare le informazioni personali e familiari[298].

L'oggetto del reato in questione sono i «*datos reservados de carácter personal o familiar de otro*». Tali dati devono essere registrati in un supporto, che può essere sia fisico che informatico[299]. I dati in questione devono essere riservati, ovvero quelli il cui accesso o conoscenza siano limitati[300]. A tal proposito, si è escluso che debbano essere qualificati come personali ai sensi della norma in questione soltanto i dati specialmente protetti[301] o comunque intimi in senso stretto, dato che altrimenti la circostanza aggravante di cui all'art. 197.5 c.p. relativa ai dati sensibili non avrebbe alcun significato[302]. Per quanto riguarda l'individuazione dei casi in cui i dati abbiano natura personale o familiare, si deve far riferimento all'art. 4 del Regolamento 2016/679/UE, c.d. GRPR, ovvero «*qualsiasi informazione riguardante una persona fisica identificata o identificabile*»[303]. Dunque, sono ricompresi nella nozione in questione dati quale il nome, il cognome, il numero di telefono, l'indirizzo *mail*, ecc. e comunque tutti i dati che permettono l'identificazione[304]. La condotta sanzionata consiste nell'impossessarsi, accedere, utilizzare o modificare i dati riservati. A

privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero».

[294] MORÓN LERMA E., *Internet y Derecho Penal: Hacking y otras Conductas Ilícitas en la Red*, cit., p. 61.

[295] DEL VALLE SIERRA LÓPEZ M., *Los delitos de descubrimiento y revelación de secretos*, cit., p. 143.

[296] MORÓN LERMA E., *Internet y Derecho Penal*, cit., p. 61; DE LA MATA BARRANCO N., *Delitos contra los sistemas de información*, cit., p. 729.

[297] ROMEO CASABONA C.M., *Los delitos de descubrimiento y revelación de secretos*, Valencia, 2004, p. 103; GALÁN MUÑOZ A., *Los ciberdelitos*, cit., p. 72.

[298] Tribunal Supremo, sez. I penale, sentenza 22 giugno 2022, n. 616.

[299] FERNÁNDEZ TERUELO J.G., *Derecho penal e internet*, cit., p. 191.

[300] ROMEO CASABONA C.M., *Los delitos de descubrimiento*, cit., p. 110; FERNÁNDEZ TERUELO J.G., *Derecho penal e internet*, cit., p. 192.

[301] MATA Y MARTÍN R.M., *Delincuencia informática*, cit., p. 134.

[302] ROMEO CASABONA C.M., *Los delitos de descubrimiento*, cit., p. 110. In giurisprudenza v. Tribunal Supremo, sez. I penale, sentenza 22 giugno 2022 n. 616; Tribunal Supremo, sez. I penale, sentenza 11 giugno 2004, n. 725; Tribunal Supremo, sez. I penale, sentenza 30 aprile 2007, n. 358.

[303] GALÁN MUÑOZ A., *Los ciberdelitos*, cit., p. 73.

[304] *Ibid*.

tal proposito, per alcuni autori l'impossessamento richiederebbe la materiale apprensione dei dati, mentre per l'accesso è sufficiente la loro mera visualizzazione[305]. Per utilizzo, invece, si intende l'impiego di tali dati, mentre modificazione e alterazione sono condotte tra loro identiche[306]. Altri autori, tuttavia, hanno osservato che in realtà è difficile distinguere nettamente le tre condotte tra di loro, essendo tutte equivalenti[307].

La norma richiede poi che il reo agisca "in danno di un terzo (o di un altro)". In merito alla natura di tale requisito, esso viene generalmente interpretato come requisito soggettivo, che descrive il dolo specifico necessario ai fini dell'integrazione del reato[308]. Alcuni autori, tuttavia, ritengono che lo stesso in realtà sia un elemento oggettivo della fattispecie[309]. Sul punto la giurisprudenza del *Tribunal Supremo* si è mostrata ambigua: da un lato ha escluso che tale inciso richieda il dolo specifico di recare un pregiudizio, ma dall'altro ha escluso anche che la norma sia un reato di evento e per la sua consumazione richieda il verificarsi di un effettivo pregiudizio per il titolare dei dati[310].

Per entrambe le ipotesi di cui all'art. 197.1 e 2, all'art. 197.6. c.p. è previsto un aumento di pena se i fatti sono commessi «*con fines lucrativos*». Non solo, ma si applica anche la sopra menzionata circostanza aggravante di cui all'art. 197-*quater* c.p. per il fatto commesso da appartenenti ad associazioni a delinquere.

È stato osservato che la regolamentazione dei delitti contro l'intimità informatica nel codice penale spagnolo è sovrabbondante, con un numero elevato di fattispecie, specialmente dopo la riforma di cui alla *Ley Orgánica* 1/2015[311]. Pertanto, per quanto riguarda l'accesso ai dati, si ritiene che se i dati non riguardino direttamente l'intimità personale, il reato applicabile sia solo quello di cui all'art. 197-*bis* c.p.[312]. Si ritiene, infatti che l'art. 197.2 e il nuovo art. 197-*bis* c.p. si distinguano tra loro perché nel primo caso l'accesso viene attuato con la finalità di scoprire un segreto altrui, perché il primo si riferisce a dati personali registrati in registri o supporti informatici, mentre il secondo ad archivi o programmi informatici e, infine, perché solo nel primo caso si richiede la violazione delle

[305] FLORES PRADA I., *Criminalidad informática*, cit., p. 108.
[306] ROMEO CASABONA C.M., *Los delitos de descubrimiento*, cit., p. 120.
[307] FERNÁNDEZ TERUELO J.G., *Derecho penal e internet*, cit., p. 190.
[308] ROMEO CASABONA C.M., *Los delitos de descubrimiento*, cit., p. 124; MORÓN LERMA E., *Internet y Derecho Penal*, cit., p. 63; FLORES PRADA I., *Criminalidad informática*, cit., p. 99.
[309] FERNÁNDEZ TERUELO J.G., *Derecho penal e internet*, cit., p. 194.
[310] Tribunal Supremo, sez. I penale, sentenza 9 dicembre 2010, n. 1084; Tribunal Supremo, sez. I penale, sentenza 23 settembre 2015, n. 532; Tribunal Supremo, sez. I penale, sentenza 22 giugno 2022, n. 616, secondo cui il pregiudizio «*se refiere al peligro de que los datos albergados en las bases de datos protegidas puedan llegar a ser conocidos por personas no autorizadas*».
[311] MUÑOZ CONDE F., *Derecho Penal*, cit., p. 292 s.
[312] *Ibid*., p. 295.

misure di sicurezza[313]. Data la diversità dei beni giuridici tutelati, si ritiene che il reato di acceso abusivo al sistema informatico possa concorrere con il successivo reato di frode informatica[314]. Qualora, però, i dati siano personali, si ritiene vi sia un concorso apparente di norme e non un concorso di reati, dato che la riservatezza informatica presenta carattere meramente strumentale rispetto all'intimità personale, con conseguente assorbimento dell'art. 197-*bis* c.p. nel successivo reato commesso riguardante l'identità personale[315].

4. L'ottenimento dell'ingiusto profitto: truffa, estorsione e frode informatica

A questo punto, dev'essere esaminata la fase dell'effettivo depauperamento della vittima, che può integrare sostanzialmente tre fattispecie, ovvero truffa, estorsione e frode informatica.

Nell'ordinamento tedesco la truffa (*Betrug*), la truffa mediante computer (*Computerbetrug*) e l'estorsione (*Erpressung*) sono tutti e tre reati classificati come *Vermögensdelikte*[316]. Allo stesso modo, anche nell'ordinamento spagnolo la truffa (*estafa*), la truffa mediante computer (*estafa informática*) e l'estorsione (*extorsión*) sono tutti classificati tra i reati contro il patrimonio[317].

4.1. La truffa

Nello *Strafgesetzbuch* il reato di truffa è previsto al § 263 StGB e sanziona colui che al fine di ottenere un illecito vantaggio patrimoniale per sé o altri danneggi la proprietà altrui creando o mantenendo un errore con falsi pretesti o distorcendo o nascondendo fatti veri[318]. Trattandosi di delitto (*Vergehen*), l'Abs. 2 prevede specificamente la punibilità del tentativo[319]. Come sopra evidenziato, bene giuridico tutelato dalla norma in questione è il

---

313 FERNÁNDEZ TERUELO J.G., *Derecho penal e internet*, cit., p. 198.
314 *Ibid*., p. 203.
315 GALÁN MUÑOZ A., *Los ciberdelitos*, cit., p. 123.
316 EISELE J., *Strafrecht Besonderer Teil*, cit. p. 1 e 242.
317 MUÑOZ CONDE F., *Derecho Penal*, cit., p. 368 ss.
318 «*Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, daß er durch Vorspiegelung falscher oder durch Entstellung oder Unterdrückung wahrer Tatsachen einen Irrtum erregt oder unterhält, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft*» (Chiunque, al fine di ottenere un vantaggio patrimoniale illecito per sé o per un terzo, danneggi la proprietà altrui creando o mantenendo un errore con false argomentazioni o distorcendo o nascondendo fatti veri, è punito con la pena detentiva non superiore a cinque anni o con la pena pecuniaria).
319 Lo *Strafgesetzbuch* al § 12 distingue tra crimini (*Verbrechen*) e delitti (*Vergehen*) a seconda che la pena detentiva prevista per il minimo edittale sia maggiore o minore di un anno. La distinzione rileva perché per la punibilità del tentativo nei delitti è necessaria un'espressa previsione legislativa, perché il tentativo di partecipazione di cui al §30 StGB è punito solo per i delitti, perché la competenza per materia del Tribunale monocratico è limitata ai delitti (§ 25 GVG), perché l'archiviazione o l'interruzione del procedimento penale per motivi di opportunità è possibile solo per i delitti e, infine, perché solo per i delitti è possibile emettere

patrimonio in senso stretto[320], ove si tutela sia la libertà di disposizione[321] quanto la mera possibilità di aumentare la ricchezza[322]. Occorre un atto di disposizione patrimoniale da parte della vittima, ove per disposizione si intende qualsiasi atto, acquiescenza od omissione che abbia un effetto diretto sulla riduzione del patrimonio[323]. Essa, inoltre, dev'essere causa diretta del danno patrimoniale per la vittima[324]. A sua volta, il danno patrimoniale richiede che si verifichi una perdita economica per la vittima[325].

Anche la truffa tedesca è un reato di evento[326], che si consuma nel momento in cui l'autore della truffa consegue l'ingiusto profitto[327]. Similmente all'art. 640 c.p. trattasi di reato a forma vincolata, ove si richiede l'affermazione di circostanze false (*falsches Vorspiegelung*) o la soppressione o la distorsione di fatti reali (*Entstellung oder Unterdrückung wahrer Tatsachen*). Dunque, qui, a differenza che della fattispecie italiana, la menzogna di per sé costituisce uno schema di comportamento fraudolento. Anche in questo caso l'altrui inganno svolge un ruolo cruciale all'interno della fattispecie. Per inganno si intende qualsiasi comportamento che oggettivamente induce in errore o crea errore, per cui influisce sulla percezione altrui[328]. Esso, però, non può limitarsi alla mera falsa dichiarazione, ma deve essere in grado di incidere sul contenuto della disposizione patrimoniale effettuata o influenzare lo scopo che la giustifica[329]. È necessario che dall'inganno scaturisca o si mantenga un errore (*Irrtum*) nella persona ingannata, errore che generalmente viene definito come mancanza di conoscenza circa un determinato fatto[330]. A tal proposito, va osservato che una parte della dottrina aderisce alla teoria vittimo-dogmatica, per cui ritiene che ai fini della responsabilità penale non è sufficiente la presenza di un nesso causale tra inganno ed errore della vittima. Dunque, il soggetto che inganna non può essere ritenuto responsabile qualora la vittima non abbia adottato tutte le necessarie misure di

ordinanza contenente le sanzioni su richiesta del pubblico ministero (§407 StPO). V. ROXIN C., GRECO L., *Strafrecht AT*, vol. I, cit., p. 375 ss.; GROPP W., SINN A., *Strafrecht AT*, cit., p. 73 s.

[320] PERRON W., *sub § 263 StGB*, in A. Schönke, H. Schröder (a cura di), *Strafgesetzbuch Kommentar*, München, XXX ed., 2019, Rn. 1.

[321] BGH, ordinanza 6 settembre 2000 - 3 StR 326/00.

[322] BGH, ordinanza 14 giugno 1991 - 3 StR 155/91.

[323] KÜHL K., *StGB § 263 Betrug*, in K. Lachner, K. Kühl, *Strafgesetzbuch Kommentar*, XXIX ed., München, 2018, Rn. 22.

[324] TIEDEMANN K., *Wirtschaftsstrafrecht*, München, 2017, p. 228.

[325] BEUKELMANN S., *StGB § 263 Betrug*, in B. von Heintschel-Heinegg (a cura di), *Beck Online Kommentar Strafgesetzbuch*, LV ed., München, 2022, Rn. 51.

[326] HEFENDEHL R., *StGB § 263 Betrug*, in V. Erb, J. Schäfer, *Münchener Kommentar zum StGB*, IV ed., München, 2022, Rn. 9.

[327] BGH, ordinanza 22 gennaio 2004 - 5 StR 415/03.

[328] KÜHL K., *StGB § 263 Betrug*, cit., Rn. 6

[329] KINDHÄUSER U., *sub § 263 StGB*, in U. Kindhäuser, U. Neumann, H. Paeffgen (a cura di), *Strafgesetzbuch*, V ed., Baden-Baden, 2017, Rn. 48.

[330] *Ibid.*, 169.

autoprotezione. Dunque, se la vittima cade in errore a causa della sua particolare credulità o per negligenza grave la frode non è punibile[331]. Non tutti, però, concordano con tale tesi e non manca chi evidenzia che le false dichiarazioni non possono essere considerate lecite per il solo fatto che la vittima vi crede per grave negligenza[332]. Quest'ultima tesi viene seguita anche dalla giurisprudenza della *Bundesgerichtshof*, secondo cui la credulità della vittima è irrilevante anche nel caso di suggestioni incredibili o promesse di impossibile compimento[333].

Con riferimento all'elemento soggettivo, a differenza della truffa italiana è richiesto il dolo specifico (*Bereicherungsabsicht*), dato che il soggetto deve agire al fine di ottenere un vantaggio patrimoniale illecito[334]. Si nega, pertanto, la sua punibilità a titolo di dolo eventuale[335].

Tale fattispecie trova applicazione alle finte vendite *online*, nonché alle *advance fee fraud* commesse su Internet: in tal caso il reato si consuma nel momento in cui il pagamento effettuato dalla persona offesa viene accreditato sul conto corrente del reo[336].

Nell'ordinamento spagnolo la fattispecie di truffa (*estafa*) fu inserita nel codice penale spagnolo con la *Ley Organica* 8/1983 del 25 giugno ed oggi è disciplinata all'art. 248 c.p.[337]. La sua struttura è molto simile al § 263 dello StGB, perché richiede quali elementi l'inganno, l'errore, l'atto di disposizione da parte della vittima, il danno patrimoniale e il dolo specifico, ovvero «*el ánimo de lucro*»[338]. Si differenzia, però, dal § 263 dello StGB e dall'omologo 640 c.p. italiano perché nella *estafa* la modalità della condotta consiste nell'uso dell'inganno. Tale inganno dev'essere "sufficiente ad indurre taluno in errore", per cui, a differenza che nel § 263 StBG, ove l'errore è elemento autonomo, nell'art. 248.1 è solamente un elemento normativo che serve a delimitare l'ambito del penalmente rilevante[339]. Inoltre, la *estafa*, a differenza della truffa italiana e della *Betrug*, richiede

---

[331] HILGENDORF E., *Zweckverfehlung und Vermögensschaden beim Betrug*, in *JuS*, 1994, p. 466 ss., p. 467; MÜHLBAUER T., *Ablisten und Verwenden von Geldautomatenkarten als Betrug und Computerbetrug*, in *NStZ*, 2003, p. 650 ss., p. 652.

[332] KINDHÄUSER U., *sub § 263 StGB*, cit., Rn. 51.

[333] BGH, sentenza 22 ottobre 1986 - 3 StR 226/86 e BGH, ordinanza 29 luglio 2009 - 2 StR 91/09.

[334] TIEDEMANN K., *Wirtschaftsstrafrecht*, cit., p. 229.

[335] EISELE J., *Strafrecht Besonderer Teil*, cit., p. 228.

[336] BGH, ordinanza 16 aprile 2014 − 2 StR 435/13.

[337] «*Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno*».

[338] PASTOR MUÑOZ N., *La determinación del engaño típico en el delito de estafa*, Madrid, 2004, p. 27. Sul concetto di «*ánimo de lucro*» v. MATA Y MARTIN R.M., *El delito de robo con fuerza en las cosas*, Valencia, 1995, p. 213 s.

[339] GÓMEZ BENITEZ J.M., *Función y contenido del error en el tipo de estafa*, in ID, *Estudios Penales*, Madrid, 2001, p. 149 ss., p. 153 s.; PASTOR MUÑOZ N., *La determinación del engaño típico en el delito de estafa*, cit., p. 27; FERNÁNDEZ-SALINERO SAN MARTIN M.A., *Las Estafas Piramidales*, cit., p. 24.

espressamente che sia la vittima a compiere l'atto di disposizione patrimoniale. Per atto di disposizione patrimoniale si intende un'azione, un atto di tolleranza o un'omissione da parte del soggetto ingannato che produca direttamente una diminuzione patrimoniale[340].

Bene giuridico protetto dalla norma in questione è il patrimonio[341], anche se alcuni autori ritengono che in realtà il bene giuridico tutelato dalla norma in questione sia anche la libertà di disposizione o comunque la buona fede nel traffico giuridico[342]. Trattasi di reato di evento, perché si richiede che la vittima subisca un pregiudizio patrimoniale[343]. Per pregiudizio patrimoniale si intende qualsiasi diminuzione economicamente valutabile, ovvero tutte le lesioni antigiuridiche del patrimonio altrui suscettibili di valutazione economica, che rendono vana la finalità economica perseguita dal soggetto passivo e che provocano un ingiusto arricchimento nei confronti del soggetto attivo[344]. Dunque, oggetto di tale reato può essere una cosa materiale, un diritto, un bene mobile o immobile[345]. Si ritiene rientrino nella nozione di patrimonio non solo i diritti reali, ma anche le obbligazioni[346]. In quest'ultimo caso, per la giurisprudenza del *Tribunal Supremo* vi è una diminuzione del patrimonio perché il soggetto passivo si trova vincolato all'obbligazione contratta, di cui deve rispondere col suo patrimonio[347]. A differenza che nella fattispecie italiana, qui il legislatore ha specificato che il danno causato può essere «*proprio o ajeno*». Pertanto, il soggetto ingannato e colui che effettua la disposizione patrimoniale devono essere la stessa persona[348], ma quest'ultima può essere diversa da colui che subisce il danno. La norma in questione, quindi, sanziona anche le c.d. truffe triangolari, nelle quali il soggetto che ha effettuato la disposizione è diverso da colui che effettivamente subisce il pregiudizio patrimoniale[349].

Come si è sopra accennato, la condotta consiste nell'utilizzo dell'inganno, ovvero un

---

[340] PASTOR MUÑOZ N., *La determinación del engaño típico*, cit., p. 172; BACIGALUPO ZAPATER E., *Falsedad documental, estafa*, cit., p. 172, secondo cui «*se debe entender toda decisión del titular del patrimonio que, mediante acción, omisión o tolerancia, conduzca directamente a una disminución del mismo*».
[341] GONZÁLEZ RUS J.J., *Los intereses económicos de los consumidores*, cit., p. 259; CHOCLÁN MONTALVO J.A., *El delito de estafa*, Barcelona, 2000, p. 38; MUÑOZ CONDE F., *Derecho Penal*, cit., p. 438; PASTOR MUÑOZ N., *La determinación del engaño típico en el delito de estafa*, cit., p. 281.
[342] ANTÓN ONECA J., voce *Estafa*, cit., p. 58.; GUTIÉRREZ FRANCÉS M.L., *Fraude informático y estafa*, cit., p. 246.
[343] MUÑOZ CONDE F., *Derecho Penal. PE*, cit., p. 442.
[344] così MARTOS NÚÑEZ J.A., *El perjuicio patrimonial en el delito de estafa*, Madrid, 1990, p. 127. In giurisprudenza v. l'importante sentenza del Tribunal Supremo, sez. I penale, 23 aprile 1992, n. 20999.
[345] ANTÓN ONECA J., voce *Estafa*, cit., p. 68; GONZÁLEZ RUS J.J., *Los intereses económicos de los consumidores*, cit., p. 258.
[346] CHOCLÁN MONTALVO J.A., *El delito de estafa*, cit., p. 165; MUÑOZ CONDE F., *Derecho Penal*, cit., p. 368.
[347] Tribunal Supremo, sez. II penale, sentenza 21 ottobre 1998, n. 1216.
[348] BACIGALUPO ZAPATER E., *Falsedad documental, estafa*, cit., p. 166.
[349] CHOCLÁN MONTALVO J.A., *El delito de estafa*, cit., p. 163.

comportamento manipolativo che incide sul processo di formazione della volontà della vittima[350]. In conseguenza dell'inganno il soggetto passivo dev'essere caduto in errore, che viene inteso come rappresentazione non corretta della realtà o come mancanza di conoscenza in merito ad una circostanza esistente[351]. Tale inganno può consistere sia nel dare informazioni false, sia nell'omettere informazioni necessarie per permettere alla vittima di decidere liberamente[352]. Anche la giurisprudenza ha fornito una nozione ampia di inganno, ovvero come qualsiasi stratagemma, frode o macchinazione[353]. L'inganno in questione deve poi essere «*antecedente*, *causante y bastante*»[354]. In particolare, deve precedere e determinare il conseguente pregiudizio patrimoniale ed essere causalmente correlato al pregiudizio patrimoniale[355]. Per quanto riguarda l'ultimo requisito, si intende che l'errore dev'essere concretamente idoneo a viziare la volontà o il consenso della vittima[356]. La mera induzione in errore, dunque, non è sufficiente ai fini della configurabilità della truffa[357]. Poiché il criterio della sufficienza dell'inganno richiama il dovere di autoprotezione della vittima[358], si ritiene che l'inganno sia sufficiente solo quando è capace di vincere i meccanismi di autoprotezione che sono esigibili da quest'ultima[359].

La giurisprudenza del *Tribunal Supremo* ha aderito alla prospettiva vittimo-dogmatica (v. *supra* cap. I, par. 8), evidenziando che il comportamento della vittima incide sul delitto di truffa, per cui il reato non è applicabile nel caso in cui le vittime siano venute meno al c.d. dovere di autoprotezione[360]. In particolare, si è negato che l'inganno sia sufficiente qualora il soggetto passivo stesso avrebbe potuto scoprire la truffa in atto mediante un'attività di verifica della realtà, se tale attività era esigibile dal soggetto[361]. Tuttavia, anche in questo caso non sono mancate sentenze discordanti[362].

---

[350] PASTOR MUÑOZ N., *La determinación del engaño típico*, cit., p. 180.
[351] BACIGALUPO ZAPATER E., *Falsedad documental, estafa*, cit., p. 171.
[352] PASTOR MUÑOZ N., *La determinación del engaño típico*, cit., p. 182.
[353] Tribunal Supremo, sez. I penale, sentenza 30 ottobre 1981, n. 5194; Tribunal Supremo, sez. I penale, sentenza 2 aprile 1982, n. 436; Tribunal Supremo, sez. I penale, sentenza 3 febbraio 1983, n. 1537; Tribunal Supremo, sez. I penale, sentenza 13 luglio 1989, n. 4234; Tribunal Supremo, sez. I, sentenza 24 novembre 1989, n. 6706; Tribunal Supremo, sez. I penale, sentenza 5 marzo 1990, n. 1982 e Tribunal Supremo, sez. I penale, sentenza 12 novembre 1990, n. 8139.
[354] Tribunal Supremo, sez. II penale, sentenza 23 aprile 1997, n. 598.
[355] CHOCLÁN MONTALVO J.A., *El delito de estafa*, cit., p. 89.
[356] *Ibid*.
[357] PASTOR MUÑOZ N., *La determinación del engaño típico*, cit., p. 119.
[358] CHOCLÁN MONTALVO J.A., *El delito de estafa*, cit., p. 120; PASTOR MUÑOZ N., *La determinación del engaño típico*, cit., p. 104 ss.
[359] CHOCLÁN MONTALVO J.A., *El delito de estafa*, cit., p. 126.
[360] Tribunal Supremo, sez. II penale, sentenza 21 settembre 1988, n. 6358.
[361] Tribunal Supremo, sez. II penale, sentenza 24 marzo 1999, n. 523; Tribunal Supremo, sez. I penale, sentenza 29 ottobre 1998, n. 1285.
[362] V. in tal senso Tribunal Supremo, sez. II penale, sentenza 27 maggio 1999, n. 836.

In merito all'identificazione dei criteri per determinare quando l'inganno sia sufficiente si sono contrapposte diverse tesi. Per alcuni deve farsi riferimento ad un criterio prevalentemente oggettivo e astratto[363]. Per altri ancora un criterio puramente soggettivo, per cui l'inganno si considera idoneo quando sia sufficiente a viziare la volontà o il consenso del soggetto passivo di quella determinata vittima, tenendo conto delle sue caratteristiche soggettive[364]. Infine, per una terza tesi, seguita dalla giurisprudenza maggioritaria, va utilizzato un criterio misto oggettivo-soggettivo, per cui l'inganno dev'essere sufficiente e proporzionato a conseguire gli obiettivi criminosi perseguiti, ma anche in funzione delle condizioni del soggetto passivo[365].

Si è posto il problema della c.d. vittima debole, ovvero, in senso ampio, la vittima c.d. normodotata che si trova in situazione di debolezza per via del mancato rispetto del dovere di veridicità da parte del reo, della vittima c.d. normodotata che si trova in situazione di debolezza per non aver attuato le necessarie misure di autoprotezione e nel caso in cui la vittima sia "debole" per caratteristiche psicofisiche (v. anziano o persona con ridotte capacità intellettive)[366]. A tal proposito, si ritiene che la soluzione sia individuare se la situazione di debolezza sia o meno rilevante per il diritto, situazione che si verifica di non imputabilità ai sensi del diritto penale[367]. In quest'ultimo caso, la mera interazione dell'autore con una vittima che si trova in situazione di debolezza comporta che l'autore del fatto abbia il dovere di supplire al deficit di conoscenza da parte della vittima[368], tant'è che si ritiene che qualora l'autore del fatto venga meno a tale dovere non vi sia truffa, ma vera e propria sottrazione[369].

---

[363] PASTOR MUÑOZ N., *La determinación del engaño típico*, cit., p. 283 s.; GALLEGO SOLER J.I., *Fundamento y límites de los deberes de autoprotección de la víctima en la estafa*, in *ADPCP*, 2005, vol. 8, p. 529 ss., p. 551; ROMERO BARRANQUERO G., *Los elementos del tipo de estafa*, Buenos Aires, 1985, p. 159. In giurisprudenza v. Tribunal Supremo, sez. II penale, sentenza 28 gennaio 1999, n. 1647.

[364] Tribunal Supremo, sez. II penale, sentenza 23 aprile 1997, n. 598; Tribunal Supremo, sez. II penale, sentenza 24 marzo 1999, n. 523.

[365] Tribunal Supremo, sez. I penale, sentenza 24 marzo 1999, n. 523; Tribunal Supremo, sez. I penale, sentenza 26 luglio 2000, n. 1349; Tribunal Supremo, sez. I penale, sentenza 2 novembre 2004, n. 1217. In dottrina v. GONZÁLEZ RUS J.J., *Los intereses económicos de los consumidores*, cit., p. 272.

[366] PASTOR MUÑOZ N., *La determinación del engaño típico*, cit., p. 244.

[367] CANCIO MELIÁ M., *Conducta de la víctima e imputación objectiva en Derecho Penal. Estudio sobre los ámbitos de responsabilidad de víctima y autor en actividades arriesgadas*, Barcelona, 1998, p. 358 ss.; PASTOR MUÑOZ N., *La determinación del engaño típico*, cit., p. 257. Va tenuto presente che nell'ordinamento spagnolo il soggetto può essere considerato non imputabile non solo in caso di anomalie o alterazioni psichiche permanenti, minore età o alterazione della percezione dalla nascita, ma anche in caso di *trastorno mental transitorio* (purché non volontariamente provocato dal soggetto col proposito di commettere il reato o la sua commissione era stata prevista o doveva essere prevista), ovvero il vizio di mente che abbia carattere temporaneo e sia dovuta ad un fattore esterno. Tra di essa si ricomprende l'intossicazione piena da alcool e sostanze stupefacenti. V. MIR PUIG S., *Derecho Penal. PS*, cit., p. 583 ss.; MUÑOZ CONDE F., GARCÍA ARÁN M., *Derecho Penal. PG*, cit., p. 345 ss.

[368] PASTOR MUÑOZ N., *La determinación del engaño típico*, cit., p. 257.

[369] CHOCLÁN MONTALVO J.A., *El delito de estafa*, cit., p. 134; PASTOR MUÑOZ N., *La determinación del engaño típico*, cit., p. 257; MUÑOZ CONDE F., *Derecho Penal. PE*, cit., p. 416 s.

Per quanto riguarda l'elemento soggettivo è dibattuto se il dolo in questione possa essere anche eventuale: per alcuni autori questo è possibile, dato che la norma richiede unicamente che il soggetto agisca col fine di profitto, non anche l'intenzione di causare un pregiudizio patrimoniale[370]. Per altri, invece, il dolo eventuale non è compatibile con la struttura della norma in questione, dato che è necessaria la volontà di ingannare la vittima, nonché di indurla ad effettuare una disposizione patrimoniale[371].

Anche in questo caso, nell'ambito applicativo della *estafa* di cui al 248 c.p. rientrano le sopra esaminate tipologie di *advance fee fraud*, perché in questo caso lo strumento informatico viene utilizzato per ingannare la vittima, la quale cade nell'errore e realizza essa stessa la disposizione patrimoniale[372]. Per quanto riguarda gli schemi truffaldini c.d. piramidali (v. supra cap. I, par. 5), anch'essi rientrano nell'ambito costitutivo della *estafa*, sussistendone tutti gli elementi costitutivi, ovvero l'inganno sufficiente e idoneo, l'errore essenziale, l'atti di disposizione patrimoniale da parte della vittima, il nesso causale tra l'inganno provocato e il danno subito dalla vittima e il fine di profitto[373]. Si evidenza poi che la commissione di truffe di questo tipo costituisce un'ipotesi di reato continuato[374]. Si ritiene, inoltre, che la fattispecie in questione sanzioni anche le truffe *online* aventi ad oggetto la creazione e l'offerta di acquisto di finte criptomonete[375].

Va però evidenziato che come sopra evidenziato la giurisprudenza del *Tribunal Supremo* ha escluso la sussistenza del reato di truffa in caso di errore grossolano (*error burdo*) da parte della vittima o in caso di assoluta mancanza di perspicacia, stupida credulità o straordinaria indolenza[376]. Questo perché, come si è esaminato sopra, la norma stessa richiede che l'inganno debba essere "sufficiente". Dunque, a differenza che nell'ordinamento italiano e tedesco, nel caso di una *advance fee fraud* si pone il problema di valutare la modalità della condotta e di verificare se la vittima sia venuta meno al suo dovere di autoprotezione. Si dovrà, dunque, esaminare secondo il criterio misto oggettivo-soggettivo i casi nei quali questo avviene.

---

[370] GALÁN MUÑOZ A., *El fraude y la estafa mediante sistemas informáticos. Análisis del artículo 248.2 c.p.*, Valencia, 2005, p. 507; CHOCLÁN MONTALVO J.A., *El delito de estafa*, cit., p. 194; ANTÓN ONECA J., voce *Estafa*, cit., p. 70.
[371] GUTIÉRREZ FRANCÉS M.L., *Fraude informático*, cit., p. 567 s.; GONZÁLEZ RUS J.J., *Los intereses económicos de los consumidores*, cit., p. 304.
[372] MIRÓ LLINARES F., *La respuesta penal al ciberfraude*, cit., p. 14.
[373] FERNÁNDEZ-SALINERO SAN MARTIN M.A., *Las Estafas Piramidales*, cit., p. 28 ss.
[374] *Ibid*., p. 21.
[375] NIETO MARTÍN A., GARCÍA-MORENO B., *Criptomonedas y derecho penal: más allá del blanqueo de capitales*, in *RECPC*, 2021, n. 23-17, p. 1 ss., p. 13 ss.
[376] Tribunal Supremo, sez. I penale, sentenza 15 marzo 2012, n. 162; Tribunal Supremo, sez. I penale, sentenza 30 marzo 2012, n. 243; Tribunal Supremo, sez. I penale, sentenza 30 aprile 2013, n. 344.

4.2. L'estorsione

Altra fattispecie significativa con riferimento alle le nuove forme di aggressione contro il patrimonio è l'estorsione. In Germania essa è punita dal § 253 StGB, che sanziona colui che utilizzi illegittimamente violenza o minaccia per costringere una persona a compiere, tollerare od omettere un atto, arrecando a quest'ultima un danno patrimoniale[377]. Trattasi anche in questo caso di reato a cooperazione artificiosa della vittima[378]. Anche in questo caso il danno causato alla vittima dev'essere un pregiudizio di carattere esclusivamente patrimoniale[379]. La fattispecie in questione è reato di evento, che si consuma quando il reo consegue l'ingiusto profitto[380]. Costituisce reato a condotta vincolata, poiché la violenza e la minaccia costituiscono il mezzo per ottenere l'ingiusto vantaggio patrimoniale[381], ove per violenza si intende l'uso della forza fisica diretto a coartare la volontà del soggetto passivo, mentre per minaccia la prospettazione di un male ingiusto[382]. La minaccia dev'essere grave, nel senso che la conseguenza negativa annunciata dev'essere in grado di indurre una persona prudente, nella situazione specifica, ad agire nel modo voluto dall'autore del reato[383]. La violenza o minaccia devono essere attuate illegittimamente: lo stesso Abs. 2 del paragrafo in questione specifica che vi è illegittimità dell'atto quando l'uso della violenza o della minaccia viene fatto per uno scopo da considerarsi riprovevole. Con riferimento all'elemento soggettivo, trattasi di reato a dolo specifico, perché è richiesto che il reo agisca al fine di profitto[384].

È controverso se la violenza possa essere diretta anche contro le cose: alcuni autori ritengono che ciò sia possibile, evidenziando che il testo della norma non richiede che la violenza sia necessariamente diretta contro le persone[385]. Altri, tuttavia, lo escludono, evidenziando che la violenza deve per forza coartare fisicamente le vittime e non è

---

[377] «*Wer einen Menschen rechtswidrig mit Gewalt oder durch Drohung mit einem empfindlichen Übel zu einer Handlung, Duldung oder Unterlassung nötigt und dadurch dem Vermögen des Genötigten oder eines anderen Nachteil zufügt, um sich oder einen Dritten zu Unrecht zu bereichern, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft*» (Chiunque, illegittimamente utilizzi violenza o minacci un male grave per costringere una persona a compiere, tollerare od omettere un atto per conseguire un ingiusto profitto per sè o per un terzo e in tal modo arrechi un danno al patrimonio della persona costretta o un terzo, è punito con la pena detentiva fino a cinque anni o con la pena pecuniaria).
[378] WITTIG P., *StGB § 253 Erpressung*, in B. von Heintschel-Heinegg (a cura di), *Beck Online Kommentar Strafgesetzbuch*, LV ed., cit., Rn. 1.
[379] JOECKS W., *Studienkommentar StGB*, München, 2012, p. 565.
[380] SANDER G.M., *StGB § 253 Erpressung*, in V. Erb, J. Schäfer (a cura di), *Münchener Kommentar zum StGB*, IV ed., 2021, Rn. 14 e 22.
[381] HAGEL K., *Raub und Erpressung nach englischem und deutschem Recht und aus rechtsvergleichender Sicht*, Berlin, 1979, p. 597.
[382] SANDER G.M., *StGB § 253 Erpressung*, cit., Rn. 8 e 10.
[383] WITTIG P., *StGB § 253 Erpressung*, cit., Rn. 4.
[384] HAGEL K., *Raub und Erpressung*, cit., p. 748.
[385] JOECKS W., *Studienkommentar StGB*, cit., p. 564.

sufficiente un effetto coercitivo meramente psicologico[386]. La questione ha estrema rilevanza per quanto riguarda i *ransomware*, dato che in questo caso la vittima non viene fisicamente coartata. Si evidenzia che però prospettare all'utente di non poter accedere ai propri dati a causa del suddetto *malware* fino a quando non pagherà una somma di denaro, o una certa quantità di criptovalute, per il suo sblocco, costituisce comunque minaccia, per cui è condotta idonea ad integrare il reato di estorsione[387]. In quest'ultimo caso vi sarà unità di azione (*Tateinheit*) tra l'estorsione e il sabotaggio informatico di cui al § 303b Abs. 1 n.1 StGB (v. *infra*, par. 6) [388].

Nell'ordinamento spagnolo l'estorsione è sanzionata nel *código penal* dall'art. 243[389]. La condotta del reato di estorsione (*extorsión*) consiste nell'obbligare un'altra persona con violenza o minaccia a realizzare o omettere un determinato atto o comportamento giuridicamente rilevante[390]. Anche qui, dunque, è necessaria la cooperazione della vittima. Per violenza si intende l'impiego di energia fisica sulle persone o sulle cose, esercitata direttamente o per mezzo di uno strumento, mentre per *intimidación* qualsiasi minaccia volta a coartare la volontà del soggetto passivo[391]. In entrambi i casi dev'essere effettiva e di intensità tale da soggiogare la volontà del soggetto passivo[392]. Oggetto dell'estorsione può essere un bene mobile, immobile, un diritto, ecc.[393], ma è sempre necessario che sia inerente al patrimonio[394]. Anche in questo caso trattasi di reato a dolo specifico (*con ánimo de lucro*)[395], che si consuma quando la vittima compie l'atto pregiudizievole, che deve avere necessariamente carattere patrimoniale[396]. Dunque, a differenza dell'omologa fattispecie italiana, non è necessario che il reo consegua effettivamente il profitto[397].

Pure in questo caso il fenomeno della *sextortion* non è specificamente regolato in una norma penale *ad hoc*, per cui può essere ricondotto a quest'ultimo reato esaminato o alla

---

386 SANDER G.M., *StGB § 253 Erpressung*, cit., Rn. 9.
387 *Ibid*., Rn. 11.
388 BGH, ordinanza 8 aprile 2021 − 1 StR 78/21; KOCHHEIM D., *Cybercrime und Strafrecht*, cit., p. 328.
389 «*El que, con ánimo de lucro, obligare a otro, con violencia o intimidación, a realizar u omitir un acto o negocio jurídico en perjuicio de su patrimonio o del de un tercero, será castigado con la pena de prisión de uno a cinco años, sin perjuicio de las que pudieran imponerse por los actos de violencia física realizados*».
390 ALONSO PÉREZ F., *Delitos Contra el Patrimonio*, cit., p. 169.
391 MUÑOZ CONDE F., *Derecho Penal. PE*, cit., p. 419.
392 *Ibid*.
393 ALONSO PÉREZ F., *Delitos Contra el Patrimonio*, cit., p. 169.
394 QUINTERO OLIVARES G., *De la extorsión*, in *Comentarios al Código Penal Español*, vol. II, VII ed., Cizur Menor, 2016, p. 69 ss., p. 71.
395 ALONSO PÉREZ F., *Delitos Contra el Patrimonio*, cit., p. 170.
396 MUÑOZ CONDE F., *Derecho Penal. PE*, cit., p. 426.
397 Tribunal Supremo, sez. I, sentenza 23 marzo 2019, n. 159. Così anche GONZÁLEZ RUS J.J., *Los delitos contra el patrimonio*, cit., p. 188.

diversa fattispecie di ricatto (*chantaje*)[398]. Quest'ultima, infatti, prevista dall'art. 171.2 c.p., sanziona colui che esige da un altro una somma o una ricompensa sotto la minaccia di rivelare o diffondere fatti riguardanti la sua vita privata o le sue relazioni familiari che non sono pubblicamente noti e che possono pregiudicare la sua reputazione, il suo credito o il suo interesse[399]. Se poi il reo non si limita a minacciare o ad ottenere il denaro dalla vittima, ma diffonde le immagini a sfondo erotico, commetterà anche il reato di cui all'art. 197.7 *código penal*, che sanziona proprio la diffusione, la rivelazione o la cessione del materiale intimo senza il consenso della vittima, il quale concorrerà con l'estorsione o il ricatto[400]. Per quanto riguarda, invece, i *ransomware*, la dottrina ritiene che la condotta del reo che chieda del denaro alle vittime in cambio del codice per sbloccare il computer vada anch'essa qualificata come estorsione, evidenziando che la vittima effettua il pagamento sotto costrizione, non avendo alcuna libertà di disposizione[401]. Tuttavia, la giurisprudenza ha qualificato la condotta di coloro che, utilizzando un *ransomware* nel quale sostenevano di aver bloccato il computer nell'ambito di un'operazione di Polizia (il c.d. *virus de la Policía*), chiedevano un riscatto per sbloccarlo come truffa continuata, in *concurso medial* con il danneggiamento informatico, sostenendo che il finto messaggio di riscatto costituisce "inganno" ai sensi dell'art. 248 c.p.[402].

---

[398] ABADÍAS SELMA A., FERNÁNDEZ ALBESA N., LEAL RUIZ R., *Ciberdelincuencia. Temas prácticos para su estudio*, A Coruña, 2021, p. 180.

[399] «*Si alguien exigiere de otro una cantidad o recompensa bajo la amenaza de revelar o difundir hechos referentes a su vida privada o relaciones familiares que no sean públicamente conocidos y puedan afectar a su fama, crédito o interés, será castigado con la pena de prisión de dos a cuatro años, si ha conseguido la entrega de todo o parte de lo exigido, y con la de cuatro meses a dos años, si no lo consiguiere*». Esso si distingue dall'estorsione perché il primo è un delitto contro la libertà personale e perché la violenza o la minaccia non raggiungono l'intensità tale richiesta dall'estorsione, sul punto v. QUINTERO OLIVARES G., *Delitos contra el patrimonio y contra el orden socioeconómico*, cit., p. 472.

[400] ABADÍAS SELMA A., FERNÁNDEZ ALBESA N., LEAL RUIZ R., *Ciberdelincuencia*, cit., p. 180.

[401] SERRANO FERRER M.P., *Derecho penal y nuevas tecnologías*, cit., p. 73; VELÁSCO NÚÑEZ E., SANCHIS CRESPO C., *Delincuencia informática. Tipos delictivos e investigación. Con jurisprudencia tras la reforma procesal y penal de 2015*, Valencia, 2019, p. 222.

[402] In tal senso Audiencia Nacional Sala de lo Penal, sez. IV del 3 marzo 2016, n. 14; Audiencia Nacional Sala de lo Penal, sez. IV del 4 luglio 2016, n. 28. Ai sensi dell'art. 77 *Código Penal* si ha *concurso medial* quando un reato costituisce l'antecedente necessario di un altro reato. Quando vi è *concurso medial* vi è concorso di reati e non concorso apparente di norme. Si ritiene che un reato sia "mezzo necessario" di un altro qualora nel caso concreto un reato non possa essere commesso senza prima commetterne anche un altro diverso. A seguito della riforma di cui alla *Ley Orgánica* n. 1/2015 cit. si prevede che la sanzione complessiva debba essere più elevata di quella prevista per il reato più grave, ma senza superare la somma delle sanzioni specifiche che sarebbero state inflitte separatamente per ciascuno dei reati, nonché i limiti previsti dall'art. 76 c.p. Sul punto v. SANZ MORAN A.J., *El concurso de normas. Aspectos de política legislativa*, Valladolid, 1986, p. 216 ss.; MIR PUIG S., *Derecho Penal. PG.*, cit., p. 677 ss.; MUÑOZ CONDE F., GARCÍA ARÁN M., *Derecho Penal. PG.*, cit., p. 443.

4.3. La frode informatica

Come si è già esaminato con riferimento al diritto italiano, anche in questo caso non tutte le nuove modalità di aggressione al patrimonio sono sanzionate dalle fattispecie tradizionali contro il patrimonio. Nell'ordinamento tedesco la riconducibilità di queste nuove manifestazioni criminose, in particolare il *phishing*, al delitto di furto (*Diebstahl* - § 242 StGB) venne sin da subito esclusa[403]. Infatti, si osservò che nel *phishing* il reo non si impossessa direttamente del denaro della vittima, ma prima ottiene i dati di autenticazione della vittima. Questi ultimi, in quanto dati, dunque oggetti immateriali e non fisici, non possono essere ricompresi nella nozione di "cose" (*Sachen*), oggetto materiale del reato di furto, la quale comprende solamente gli oggetti fisici[404]. Né ad oggi risulta esservi stato qualche tentativo di interpretare diversamente la nozione di *Sachen* in modo tale da ricomprendervi anche i dati, come invece è accaduto in Italia (v. *supra* cap. II, par. 9). Le medesime difficoltà si registrarono anche in Spagna, poiché anche nel *Código Penal* l'oggetto materiale del reato di furto è una *cosa mueble ajena*, concetto ristretto alle cose materiali delle quali è possibile la sottrazione e l'apprensione fisica[405]. Per cui si è esclusa la riconducibilità delle nuove manifestazioni criminose, ove oggetto del reato non è il denaro contante, ma moneta contabile, dunque immateriale, alle fattispecie tradizionali quali furto e truffa[406]. Nonostante ciò, in passato furono dei tentativi da parte della giurisprudenza del *Tribunal Supremo* di espandere l'ambito applicativo delle fattispecie già in vigore per ricomprendervi anche i nuovi fenomeni criminosi. Emblematico è l'esempio dell'indebito utilizzo di carte di credito, qualificato come furto con violenza sulle cose dopo aver equiparato tali strumenti elettronici alla "chiave" di cui agli artt. 238 e 239 c.p.[407], non senza critiche da parte di alcuni autori[408]. Inoltre, vi era comunque un settore della dottrina che riteneva che le norme penali già in vigore, in particolare la truffa comune, fossero già idonee

[403] HANSEN D., *Strafbarkeit des Phishing*, cit., p. 48.
[404] WITTIG P., *sub § 242 StGB*, in B. von Heintschel-Heinegg (a cura di), *Beck Online Kommentar Strafgesetzbuch*, VIII ed., München, 2022, Rn. 4-4.2, disponibile *online* al sito https://beck-online.beck.de; MAIWALD M., *Der Zueignungsbegriff im System der Eigentumsdelikte*, Heidelberg, 1970, p.117 ss.; NIETHAMMER E., *Lehrbuch des Besonderen Teils des Strafrechts*, Tübingen, 1950, p. 227.
[405] Va evidenziato che nell'ordinamento spagnolo, analogamente a quello tedesco, non esiste una definizione di cosa mobile analoga a quella di cui al co. 2 dell'art. 624 c.p.
[406] ROMEO CASABONA C.M., *Poder informático y seguridad jurídica*, cit., p. 85. GONZÁLES RUS J.J., *Protección penal de sistemas, elementos, datos, documentos, programas informáticos*, in *RECPC*, 1999, n. 1, p. 1 ss., p. 18; CHOCLÁN MONTALVO J.A., *Estafa por computación y criminalidad económica*, cit., p. 1078.
[407] V. *ex multis* Tribunal Supremo, sentenza 21 marzo 1988; Tribunal Supremo, sentenza 6 marzo 1989; Tribunal Supremo, 27 febbraio 1990. STS 392/07, 1680/03.
[408] MATA Y MARTÍN R.M., *Estafa Convencional, Estafa Informática y Robo en el Ámbito de los Medios Electrónicos de Pago. El Uso Fraudulento de Tarjetas y otros Instrumentos de Pago*, Cizur Menor, 2007, p. 125.

a ricomprendere nel loro ambito applicativo le nuove manifestazioni criminose sopra esaminate[409].

Per ovviare alle difficoltà evidenziate, furono introdotte le specifiche norme penali per combattere le frodi informatiche.

Nell'ordinamento tedesco, il delitto di truffa mediante computer (*Computerbetrug*) [410], l'equivalente della frode informatica italiana, fu introdotto al § 263a dello *Strafgesetzbuch* dalla seconda legge per la lotta contro la criminalità economica (*2. WiKG*). Prevalse la scelta di introdurre una specifica previsione di reato e non di limitarsi ad una mera modifica o integrazione della truffa comune, tecnica legislativa che ha avuto quale conseguenza quella di fornirle maggiore autonomia giuridica[411]. Come sopra evidenziato, tale reato fu collocato accanto alla truffa tradizionale, ad essa ritenuta analoga come oggetto di tutela. Analogamente a quanto avviene in Italia, infatti, non mancano coloro che a tutt'oggi ritengono che la differenza tra la truffa mediante computer e la truffa tradizionale consista semplicemente nel fatto che in quest'ultima l'inganno viene rivolto ad una persona, mentre nella *Computerbetrug* esso coinvolge il sistema di elaborazione dei dati[412]. Si tratta di un reato di evento: la norma richiede il verificarsi di un danno al patrimonio altrui causato dall'indebita interferenza sul processo di elaborazione dei dati dello strumento informatico[413]. A differenza della frode informatica *ex* art. 640-*ter* c.p., però, questa fattispecie è a dolo specifico, perché il reo deve agire col fine di trarre un ingiusto profitto[414].

È un reato a forma vincolata, perché l'indebita interferenza prevista dalla norma deve avvenire secondo una delle seguenti quattro modalità di esecuzione: configurazione errata del programma, utilizzo di dati errati o incompleti, uso non autorizzato di dati, altra indebita interferenza nel processo di elaborazione. Per "configurazione" deve intendersi qualsiasi

---

[409] V. A tal proposito GUTIÉRREZ FRANCÉS M.L., *Fraude informático y estafa*, cit., p. 582 ss.

[410] «*Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, daß er das Ergebnis eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf beeinflußt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft*» (Chiunque, al fine di ottenere un vantaggio patrimoniale illecito, danneggia il patrimonio altrui influenzando il risultato di un'operazione di elaborazione dati attraverso una configurazione errata di un programma, l'uso di dati errati o incompleti, l'uso non autorizzato di dati o altra indebita interferenza nel corso del processo di elaborazione, è punito con la pena detentiva non superiore a cinque anni o con la pena pecuniaria).

[411] Per approfondire la genesi della *Computerbetrug* v. PICOTTI L., *Studi di diritto penale dell'informatica*, cit., p. 48.

[412] BORGES G., SCHWENK J., STUCKENBERG C., WEGENER C., *Identitätsdiebstahl und Identitätsmissbrauch im Internet*, cit., p. 210.

[413] SCHMIDT R., *sub. § 263a Computerbetrug*, in B. Von Heintschel-Heinegg (Hrsg), *Beck-Online Kommentar StGB*, XLVII ed., München, 2020.

[414] *Ibid*.

modifica di un programma informatico, sia dall'inizio della sua progettazione iniziale così come attraverso la successiva manipolazione di un programma esistente, sia inserendo, modificando, sovrapponendo o eliminando programmi o parti di programma[415]. L'"utilizzo" consiste in qualsiasi introduzione di dati nel processo di elaborazione, non solo se esso è già iniziato, ma anche se è stato solo avviato con l'inserimento dei dati[416]. Sulla delimitazione del concetto di "uso non autorizzato" di dati informatici la dottrina ha sviluppato tre diverse tesi: la prima è quella dell'interpretazione soggettiva, per cui si ha utilizzo non autorizzato di dati quando questi sono introdotti nel sistema informatico contro la volontà del titolare, così che, come accade in modo analogo nel delitto tradizionale di truffa, il dispositivo sia "ingannato" da questi dati[417]. È evidente, tuttavia, come questa tesi sia poco persuasiva, dal momento che il sistema non può essere "ingannato", limitandosi ad eseguire le funzioni richieste da parte del suo utilizzatore. La seconda, denominata dell'interpretazione specificamente informatica (*Computerspezifische Auslegung*) è un'interpretazione restrittiva, secondo la quale vi è abuso solo se nel corso dell'elaborazione vi è un controllo sull'autorizzazione all'utilizzo dei dati, quindi solo ove per entrare nel programma sia necessario inserire un codice di accesso[418]. Anche tale teoria non va esente da critiche, in quanto si osserva che in tal modo si finisce per escludere dall'ambito applicativo della norma in questione proprio l'utilizzo abusivo di codici d'accesso altrui illegittimamente carpiti, privandola di significato[419]. L'ultima tesi (*betrugsnahe Auslegung*), ad oggi maggioritaria[420], tiene conto della similitudine strutturale tra la fattispecie della truffa e quella della frode informatica: dal momento che in quest'ultima fattispecie la condotta fraudolenta sostituisce l'inganno tipico della truffa, l'uso di dati si considera "non autorizzato" solo ove abbia come effetto quello di ingannare una persona fisica. In questo modo l'azione è diretta contro l'operatore, cui viene nascosta la mancanza di autorizzazione[421]. Per quanto riguarda invece la locuzione «*altra indebita interferenza*», essa svolge una funzione di chiusura che permette di punire altre modalità di esecuzione della condotta non elencate precedentemente, quali, ad esempio, le cosiddette manipolazioni di *output*, che influiscono direttamente sul "risultato" del processo di elaborazione dei dati o sulla registrazione dei risultati

[415] KINDHÄUSER U., *§ 263 a StGB Computerbetrug*, in U. Kindhäuser, U. Neumann e H. Ullrich Paeffgen (Hrsg.), *Strafgesetzbuch-Nomos Kommentar*, V ed., München, 2017.
[416] SCHMIDT R., *sub. § 263a Computerbetrug*, cit.
[417] KINDHÄUSER U., *sub StGB § 263 a Computerbetrug*, cit.
[418] *Ibid*.
[419] MÜHLBAUER T., *StGB § 263 a Computerbetrug*, in AA.VV., *Münchener Kommentar zum StGB*, III ed., München, 2019, par. 48.
[420] WACHTER M., *Grundfälle zum Computerbetrug*, in *JuS*, 2017, p. 723 ss., p. 726.
[421] SCHMIDT R., *sub. § 263a Computerbetrug*, cit.

dell'operazione di elaborazione dati (ad esempio impedendo la stampa) oppure le manipolazioni alla *consolle*, che forniscono al reo opzioni di comando ulteriori [422]. La norma richiede poi che le quattro condotte descritte influenzino il risultato dell'operazione di trattamento dei dati, per cui è necessario verificare la presenza di un nesso di causalità tra l'avvenuta interferenza del risultato dell'elaborazione e il processo di manipolazione del sistema informatico[423].

Questa fattispecie è largamente utilizzata nell'ordinamento tedesco per punire le frodi informatiche che vengono realizzate tramite la violazione dei sistemi di *home banking*, ovvero nei casi in cui il reo effettui trasferimenti *online* contro la volontà del titolare del conto (utilizzando, ad es., il suo PIN, i codici d'accesso precedentemente sottratti, ecc.)[424]. Analogamente a quanto riferito per l'ordinamento italiano, anche qui sono stati manifestati dei dubbi sull'applicabilità della *Computerbetrug* al fenomeno del *phishing* classico. Infatti, una parte della dottrina tedesca ritiene che il successivo utilizzo dei dati raccolti con questa modalità sia punito dal § 263a StGB in quanto si tratterebbe di uso non autorizzato di dati[425], ed addirittura ipotizza che il semplice invio di *e-mail* di *phishing* possa essere di per sé punibile come tentativo di una frode informatica, anche se su quest'ultima opinione la giurisprudenza non è concorde[426]. Altri autori, invece, ritengono che questa manifestazione criminosa rientri nelle ipotesi punite dalla fattispecie di truffa comune di cui al § 263 StGB, evidenziando che il *deceptive phishing* non consiste in una manipolazione di dati, bensì nella creazione di siti o *e-mail* contraffatti, affinché il destinatario del messaggio vi acceda o segua le istruzioni ivi contenute credendo che siano autentici[427].

Anche in questo caso valgono le osservazioni già svolte con riferimento alla normativa italiana sull'inopportunità di un'aprioristica presa di posizione per la

---

[422] *Ibid*.
[423] MÜLLER W., *Aktuelle Probleme des § 263a StGB*, Frankfurt am Main, 1999, p. 168.
[424] KINDHÄUSER U., sub *StGB § 263 a Computerbetrug*, cit.
[425] JAHN M., *Strafrecht AT und BT: Versuchter Computerbetrug durch Phishing Zum unmittelbaren Ansetzen beim versuchten Computerbetrug*, in *JuS*, 2012, p. 1135 ss., p. 1136.; POPP A., "*Phishing", "Pharming" und das Strafrecht*, in *MMR*, 2006, p. 84 ss., p. 84 s.
[426] «*Hat ein Täter widerrechtlich Konto-, Identifikations- und Transaktionsnummern sowie Zugangscodes von anderen Benutzern des Internet mittels Phishing erlangt, liegt ein Ansetzen zur Verwirklichung des Straftatbestands des Computerbetrugs i.S.d. § StGB § 22 erst dann vor, wenn er diese Daten verwendet, indem er sie z.B. in den Computer eingibt, um so eine von dem tatsächlich Berechtigten nicht autorisierte Überweisung zu tätigen*» (Se l'autore del reato ha acquisito illegalmente i numeri del conto corrente, d'identificazione e transazione, nonché i codici di accesso di altri utenti *Internet* tramite il *phishing*, esiste un tentativo di realizzazione di una frode informatica ex art. i.S.d. § StGB § 22 solo quando il reo utilizza questi dati, per esempio in un accesso abusivo, in modo da effettuare effettivamente un trasferimento di dati da parte di persona non autorizzata) così KG, ordinanza 2 maggio 2012 - (3) 121 Ss 40/12 (26/12), in *MMR*, 2012, p. 845 ss.
[427] GRAF J.P., *"Phishing"*, cit., p. 130.

configurabilità dell'una piuttosto che dell'altra fattispecie. Pure la dottrina tedesca, infatti, è orientata per una bipartizione, ritenendo che si configuri il reato di truffa nel caso in cui diminuzione patrimoniale sia il risultato diretto di un atto umano comune e la frode informatica se essa sia il risultato diretto di un'operazione di elaborazione dati[428].

Nel codice penale spagnolo, a seguito della *Ley Orgánica* 14/2022 la frode informatica viene sanzionata all'art. 249.1 lett. a) c.p.[429]. Essa fu introdotta proprio allo scopo di sanzionare quelle frodi nelle quali il trasferimento patrimoniale era conseguenza della manipolazione del sistema informatico o del processo di elaborazione dati e non dell'errore della vittima causato da inganno[430].

In quest'ultimo caso, a differenza di quanto avviene in Italia e Germania, la frode informatica inizialmente non fu collocata in una distinta e autonoma fattispecie, ma fu inserita nello stesso articolo che sanziona la truffa (*estafa*) comune. Lo stesso incipit della frode informatica tutt'oggi recita "allo stesso modo si considerano colpevoli di truffa". Per questo motivo, la sua autonomia rispetto a quest'ultima fattispecie è stata estremamente controversa[431]. Va però evidenziato che a seguito della menzionata *Ley Orgánica* 14/2022 la collocazione della frode informatica è mutata, per cui oggi è presente nel nuovo e riformato art. 249 c.p., ovvero in un articolo autonomo e diverso rispetto a quello della truffa comune, la quale, invece, resta regolata dall'art. 248 c.p. Oggi, dunque, non appare esservi dubbio in merito all'autonomia della frode informatica rispetto alla fattispecie di truffa comune.

Anche qui le differenze tra quest'ultima fattispecie e la frode informatica sono significative. Infatti, in luogo dell'induzione in errore tramite inganno, la condotta vietata consiste nella manipolazione informatica o artifizio simile. Inoltre, a differenza di Italia e

---

[428] HASSEMER I.M., *Strafrecht im Bereich der Informationstechnologien*, in A. Auer-Reinsdorff, I. Conrad (a cura di), *Handbuch IT- und Datenschutzrecht,* München, III ed., 2019, par. 254; MÜHLBAUER T., *sub § 263a StGB,* cit., par. 97.

[429] «*También se consideran reos de estafa: a)* los *que, con ánimo de lucro, obstaculizando o interfiriendo indebidamente en el funcionamiento de un sistema de información o introduciendo, alterando, borrando, transmitiendo o suprimiendo indebidamente datos informáticos o valiéndose de cualquier otra manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro*».

[430] V. FERNÁNDEZ TERUELO J.G., *Derecho penal e internet,* cit., p. 46, il quale però evidenzia che la norma non fu introdotta con l'obiettivo di sanzionare frodi commesse attraverso *Internet*, ma piuttosto per sanzionare quei casi in cui i sistemi bancari o i terminali di pagamento (POS) vengono indebitamente utilizzati da un dipendente o un terzo per effettuare trasferimenti a loro favore o a favore di un terzo.

[431] Per alcuni autori si trattava di fattispecie autonoma, v. FARALDO CABANA P., *Las nuevas tecnologías,* cit., p. 85.; GALÁN MUÑOZ A., *El fraude,* cit. p. 791 ss.; SUÁREZ GONZÁLEZ C., *sub Art. 248,* in G. Rodriguez Mourullo (dir.), A. Jorge Barreiro (coord.), *Comentarios al código penal*, cit., p. 708 ss., p. 710, il quale sostiene che «*Su ubicación sistematica es, empero, criticable. Lo corretto hubiera sido crear una figura autónoma no incardinada a la estafa*». Per altri, invece, di un'ipotesi qualificata della truffa, v. GUTIÉRREZ FRANCÉS M.L., *Delincuencia económica e informática en el nuevo Código Penal*, in *CDJ*, 1996, n. 11, p. 247 ss., p. 270. Per una sintesi delle diverse posizioni v. GALÁN MUÑOZ A., *El fraude*, cit., p. 285 ss.

Germania, al posto di indurre la vittima a realizzare un atto di disposizione patrimoniale, nella frode informatica spagnola si sanziona l'ottenimento un trasferimento non consensuale di un valore patrimoniale attivo (*conseguir una transferencia no consentida de un activo patrimonial*), similmente all'aggravante di nuova introduzione di cui al co. 2 all'art. 643-*ter* c.p. (v *supra* cap. III, par. 2.2), che deve avvenire «*en perjuicio de otro*». La formula in questione appare essere la più funzionale rispetto a quelle sinora esaminate, perché il "valore patrimoniale attivo" è formula ampia, che consente di ricomprendere qualsiasi tipologia di valore economico, sia esso monetario o valuta virtuale, senza necessità di continue modifiche della fattispecie per adattarla ai nuovi strumenti di accumulo della ricchezza. Anche in questo caso trattasi di reato a forma vincolata, dato che pregiudizio patrimoniale deve avvenire a seguito delle condotte espressamente indicate dalla norma in questione[432].

Bene giuridico tutelato dalla norma in questione è sempre il patrimonio[433], anche se anche in questo caso qualche autore qualifica il reato in questione come plurioffensivo[434].

La condotta della *estafa informática* consiste nell'uso della manipolazione informatica o "altro simile artificio" (*otro artificio semejante*), che sono tra loro alternative[435]. Anche in questo caso, analogamente all'art. 640-*ter* c.p., le modalità commissive sono descritte in modo ampio e generale, senza una numerazione esaustiva[436]. Per manipolazione informatica si intende qualsiasi alterazione del corretto funzionamento del sistema in qualsiasi fase del processo o trattamento informatico che causi un indebito trasferimento di un attivo patrimoniale[437]. Si considera, dunque, come manipolazione informatica non solo qualsiasi condotta che incida sul processo di elaborazione dei dati in corso, ma anche qualsiasi introduzione di dati (*imput*) o qualsiasi alterazione del risultato finale senza intervenire nel processo di elaborazione (*output*)[438]. A tal proposito, la stessa

---

[432] ANARTE BORRALLO E., *Incidencia de las nuevas tecnologías en elsistema penal. Aproximación al Derecho Penal en la sociedad de la información*, in *Derecho y conocimiento. Anuario jurídicosobre la sociedad de la información*, 2001, vol. 1, p. 191 ss., p. 236 s.

[433] GALÁN MUÑOZ A., *El fraude*, cit., p. 269 e 282; CHOCLÁN MONTALVO J.A., *El delito de estafa*, p. 35; DOPICO GÓMEZ-ALLER J., *Estafas y otros fraudes en el ámbito empresarial*, cit., p. 231.

[434] ROVIRA DEL CANTO E., *Delincuencia informática y fraudes informáticos*, Granada, 2002, p. 562.

[435] GALÁN MUÑOZ A., *El fraude*, cit., p. 559.

[436] *Ibid*.

[437] ROMEO CASABONA C.M., *Poder informático*, cit., p. 47; MATA Y MARTÍN R.M., *Delincuencia informática y derecho penal*, Madrid, 2001, p. 48.; GALÁN MUÑOZ A., *Los ciberdelitos*, cit., p. 144. Per FARALDO CABANA P., *Las nuevas tecnologías*, cit., p. 89, invece, la manipolazione informatica coincide con la condotta descritta dall'art. 3 della decisione quadro 2001/413/JAI, per cui consiste nell'introduzione, alterazione, cancellazione o soppressione indebita di dati informatici, nonché nell'indebita interferenza nel funzionamento di un programma o sistema informatico.

[438] GALÁN MUÑOZ A., *El fraude y la estafa*, cit., p. 561.; MIRÓ LLINARES F., *La respuesta penal al* ciberfraude, cit., p. 14. In giurisprudenza v. Tribunal Supremo, sez. I penale, sentenza 20 novembre 2001, n. 2175 e Tribunal Supremo, sez. I penale, sentenza 20 giugno 2006, n. 692.

giurisprudenza ha precisato che vi è manipolazione informatica anche nel caso in cui il reo non abbia l'autorizzazione all'utilizzo del sistema informatico o lo utilizzi in modo scorretto[439].

La seconda modalità di condotta descritta consiste nell'utilizzo di "altro simile artificio". L'artificio in questione dev'essere simile alla manipolazione informatica, per cui deve per forza essere relativo ad un elemento informatico[440]. Trattasi di una clausola di chiusura, che serve a non creare vuoti di punibilità per i casi in cui non ci sia manipolazione informatica in senso stretto e non rendere la norma obsoleta rispetto alla rapida evoluzione delle nuove tecnologie[441]. La presenza di tale clausola espressa di chiusura, che nella frode informatica italiana è assente, rende tale norma simile alla *Computerbetrug* tedesca. Il rapporto tra quest'ultima modalità della condotta e la manipolazione informatica è di difficile individuazione e si è lungo discusso in dottrina su quali potessero essere i criteri per delineare una linea di demarcazione. Anche in questo caso si è però ritenuto che, data la notevole estensione del concetto di manipolazione informatica, le due modalità della condotta descritte non siano realmente alternative e che la modalità dell'uso di artificio simile sia in realtà priva di contenuto e in sostanza inapplicabile[442].

Nonostante ciò, a seguito della *Ley Orgánica* 14/2022 alle condotte già previste sono state aggiunte quelle di ostacolo, interferenza indebita nel funzionamento del sistema informatico, nonché l'introduzione, alterazione, cancellazione, trasmissione o soppressione indebita di dati informatici. Tale aggiunta, che peraltro ricalca integralmente il testo dell'art. 6 della direttiva 2019/7137UE, è assolutamente superflua, dato che, come si è esaminato, tali condotte già potevano essere ricomprese nel concetto di manipolazione informatica.

La manipolazione informatica deve poi produrre un trasferimento di un valore patrimoniale attivo. Per quanto riguarda la nozione di trasferimento di un attivo patrimoniale, essa viene intesa sia in senso amplio come il mero trapasso di un valore attivo patrimoniale da un titolare ad un altro, sia come la realizzazione di un determinato processo che causi il trasferimento elettronico di fondi[443]. Tale trasferimento, dunque, rappresenta l'equivalente dell'atto di disposizione del reato di truffa tradizionale[444]. Il trasferimento dev'essere "non

[439] Tribunal Supremo, sez. I penale, sentenza 21 dicembre 2004, n. 1476; Tribunal Supremo, sez. I penale, sentenza 12 giugno 2007, n. 533.
[440] FARALDO CABANA P., *Las nuevas tecnologías,* cit., p. 97 s.; MATA Y MARTÍN R.M., *Estafa convencional,* cit., p. 94.
[441] MATA Y MARTÍN R.M., *Delincuencia informática,* cit., p. 48.
[442] GALÁN MUÑOZ A., *Los ciberdelitos en el ordenamiento español*, Barcelona, 2019, p. 145.
[443] GALÁN MUÑOZ A., *El fraude y la estafa,* cit., p. 591 ss.
[444] MATA Y MARTÍN R.M., *Delincuencia informática,* cit., p. 53.

consentito", elemento che differenzia la fattispecie in questione rispetto alla truffa comune e che evidenzia che la condotta descritta è in realtà surrettizia e che il trasferimento deve avvenire senza il consenso del titolare[445]. La frode informatica, dunque, assomiglia più al furto che alla truffa comune[446].

Oggetto materiale del reato in questione, dunque, è qualsiasi valore che però non necessariamente è incorporato in un oggetto materiale[447]. In particolare, si ritiene costituiscano attivo patrimoniale tutte quelle poste attive rappresentate in annotazioni o registri informatici la cui alterazione può provocare il trasferimento del valore economico che rappresentano a favore di un terzo, con la conseguente perdita della capacità di disposizione sugli stessi di cui il titolare godeva[448]. Per alcuni autori tale nozione ricomprende tutti gli strumenti di pagamento utilizzati nella rete di telecomunicazioni senza che vi sia coincidenza temporale tra il pagamento e la sua contabilizzazione, quali ad esempio le carte di credito, nonché la moneta elettronica[449]. Per altri ancora essa ricomprende non solo beni, ma anche servizi[450]. Tuttavia, altri autori dubitano che ciò sia possibile, dato che nella formulazione della norma non si fa riferimento ad alcuna attività umana[451].

Anche in questo caso si tratta di un reato di evento, poiché occorre che il trasferimento produca un pregiudizio patrimoniale, da intendersi come una diminuzione del patrimonio, secondo un confronto della situazione del soggetto attivo prima e dopo l'atto di disposizione[452]. Inoltre, esattamente come nella frode informatica italiana, l'evento è duplice e consiste nell'indebito arricchimento dell'autore con conseguente lesione patrimoniale causata alla vittima[453].

Trattasi di reato comune[454] e, analogamente alla *Computerbetrug* tedesca, punito a titolo di dolo specifico, dato che il reo deve agire con «*ánimo de lucro*»[455]. Ulteriore dato comune a tutti e tre gli ordinamenti esaminati, italiano, tedesco e spagnolo, è che la truffa e la frode informatica nelle rispettive ipotesi base presentano pene identiche.

---

[445] FARALDO CABANA P., *Las nuevas tecnologías*, cit., p. 86. Per altri autori, invece, la clausola in questione è superflua, in tal senso v. SUÁREZ GONZÁLEZ C., *sub art. 248*, in G. Rodriguez Mourullo (dir.), A. Jorge Barreiro (coord.), *Comentarios al código penal*, cit., p. 711.
[446] GALÁN MUÑOZ A., *El fraude y la estafa*, cit., p. 616.
[447] MATA Y MARTÍN R.M., *Estafa Convencional*, cit., p. 97.
[448] GALÁN MUÑOZ A., *El fraude y la* estafa, cit., p. 612 s.
[449] MATA Y MARTÍN R.M., *Estafa Convencional*, cit., p. 98.
[450] GONZÁLES RUS J.J., *Protección penal de sistemas*, cit., p.
[451] MATA Y MARTÍN R.M., *Delincuencia informática*, cit., p. 53.
[452] ANARTE BORRALLO E., *Incidencia de las nuevas tecnologías en elsistema penal*, cit., p. 236.
[453] MATA Y MARTÍN R.M., *Delincuencia informática*, cit., p. 53.
[454] MATA Y MARTÍN R.M., *Estafa Convencional*, cit., p. 142.
[455] GALÁN MUÑOZ A., *Los ciberdelitos en el ordenamiento español*, cit., p. 169.

Anche in questo caso, per quanto riguarda il *pharming*, non ci sono dubbi in merito alla sua configurabilità quale frode informatica ex art. 249.1 lett. a) c.p.[456]. Con riguardo al *phishing* classico, invece, vi è chi sostiene che lo stesso integri la fattispecie di *estafa común* e non di *estafa informática*, perché difetta l'elemento della manipolazione informatica[457]. Però vi è chi evidenzia che la *estafa común* richiede espressamente che sia la vittima ad effettuare la disposizione patrimoniale, mentre nel caso del *phishing* una volta ottenute le credenziali della vittima il reo non ha più alcuna necessità di interagire con quest'ultima ed effettua autonomamente la disposizione patrimoniale. Pertanto, difetta l'elemento oggettivo dell'inganno, così come l'errore che ha determinato la disposizione patrimoniale[458], per cui lo qualifica come frode informatica[459]. Per quanto riguarda, invece, l'accesso al sistema di *home banking* con le credenziali del titolare del conto corrente per effettuare disposizioni di pagamento in pregiudizio di quest'ultimo, una parte della dottrina non ritiene che esso rientri nell'ambito applicativo dell'art. 249.1 lett. a), evidenziando che in questo caso non vi è né manipolazione informatica, né l'utilizzo di un artificio simile[460]. La giurisprudenza del *Tribunal Supremo*, invece, ritiene che il *phishing* classico sia punibile quale frode informatica[461].

Inizialmente l'indebito utilizzo di carta di credito non era pacificamente riconducibile alla frode informativa. Vi era, infatti, la difficoltà a qualificare l'utilizzo di dati autentici senza l'autorizzazione del titolare, in particolare quelli relativi alle carte di credito, come manipolazione informatica, dato che in questo caso non si verifica alcuna interferenza nel funzionamento del sistema[462]. Per questo motivo, il legislatore spagnolo ha deciso di intervenire con la *Ley Orgánica* 5/2010 cit. inserendo una nuova lett. c) all'art. 248.2. c.p., che sanziona l'utilizzo di carte di credito, di debito, di *traveller's cheque* o dei dati in essi contenuti per effettuare transazioni di qualsiasi tipo a danno del titolare della carta o di terzi. A seguito della *Ley Orgánica* 14/2022 tale disposizione è oggi contenuta nel novellato art. 249.1 lett. b) c.p.[463]. Inoltre, l'oggetto del reato è stato ampliato tramite l'aggiunta di

[456] FARALDO CABANA P., *Las nuevas tecnologías,* cit., p. 92; MIRÓ LLINARES F., *La respuesta penal al ciberfraude,* cit., p. 29.
[457] MATA Y MARTÍN R.M., *Delincuencia informática,* cit., p. 57.
[458] FARALDO CABANA P., *Las nuevas tecnologías,* cit., p. 91; FERNÁNDEZ TERUELO J.G., *Derecho penal e internet,* cit., p. 46.
[459] MIRÓ LLINARES F., *La respuesta penal al ciberfraude,* cit., p. 29 s.
[460] DOPICO GÓMEZ-ALLER J., *Estafas y otros fraudes en el ámbito empresarial,* cit., p. 230 s.
[461] Tribunal Supremo, sez. I, sentenza 26 ottobre 2018, n. 509; Tribunal Supremo, sez. I, sentenza 12 giugno 2007, n. 3935;
[462] FARALDO CABANA P., *Las nuevas tecnologías,* cit., p. 92.
[463] «*Los que, utilizando de forma fraudulenta tarjetas de crédito o débito, cheques de viaje o cualquier otro instrumento de pago material o inmaterial distinto del efectivo o los datos obrantes en cualquiera de ellos,*

"qualsiasi strumento di pagamento materiale o immateriale diverso dai contanti".

L'ampia formulazione della norma comporta la sua applicabilità nel caso di qualsiasi utilizzo dei suddetti oggetti che causi un pregiudizio patrimoniale per il titolare degli stessi o per un terzo[464]. Dunque, seguendo il principio di specialità, nell'ambito applicativo della norma in questione sono ricomprese tutte quelle forme di trasferimento non consentito di un valore patrimoniale attivo realizzate tramite l'impiego in un sistema informatico di dati di carte di credito, che, dunque, non rientrano nell'ambito applicativo dell'art. 249.1 lett. a) c.p., nonostante l'ampia definizione di manipolazione informatica[465]. Vi è chi ha criticato la formulazione piuttosto ampia della norma ed evidenzia che sia necessario quantomeno che le operazioni realizzate siano non consentite o comunque non autorizzate[466].

Per quanto riguarda la configurabilità del concorso tra fattispecie, nell'ordinamento tedesco, esattamente come avviene in Italia, la *Computerbetrug* viene considerata speciale rispetto alla truffa comune, per cui i due reati non concorrono tra di loro[467]. Con riferimento alle diverse fasi del *phishing* si può configurare unità di azione (*Tateinheit*) tra i reati esaminati di cui ai §§ 202a, 263a e 269 StGB[468], per cui, ai sensi del § 52 StGB, trova applicazione la pena prevista per il solo reato più grave, che assorbe tutte le altre pene. Per quanto riguarda, invece, il rapporto tra i reati che vengono ad evidenza nella prima e nella seconda fase dei *phishing attacks*, il § 202c StGB è considerato un reato presupposto, per cui in caso di perfezionamento dei reati di cui ai §§ 202a e 202b si considera assorbito[469]. Il § 202b StGB, invece, è dotato di clausola di sussidiarietà, per cui si applica solamente se il fatto non integra il diverso reato di spionaggio di dati di cui al § 202a, ovvero non è stata superata una misura di sicurezza per l'accesso al sistema informatico[470]. Infine, con riferimento al § 202d (*Datenhehlerei*), si può configurare il concorso materiale coi reati di cui ai §§ 263 e 263a, mentre unità di azione coi reati dei §§ 202c e 269[471].

Nell'ordinamento spagnolo, invece, si ritiene che tra la frode informatica consumata

---

realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero». Evidenzia PRIETO DEL PINO A.M., *Criminal offences against property,* cit., p. 95, che il riferimento ai *travel cheques* era già obsoleto al momento dell'introduzione della norma e che ciò è dovuto al ritardo col quale il legislatore spagnolo ha recepito la decisione quadro del 2005 sugli strumenti di pagamento.

[464] GALÁN MUÑOZ A., *Los ciberdelitos,* cit., p. 159.

[465] *Ibid*., p. 160.

[466] DOPICO GÓMEZ-ALLER J., *Estafas y otros fraudes en el ámbito empresarial,* cit., p. 232.

[467] SCHMIDT R., *sub § 263a StGB,* cit., par. 53.

[468] *Ibid.*, par. 55.

[469] WEIDEMANN M., *sub § 202c StGB,* cit., par. 13.

[470] WEIDEMANN M., *sub § 202b StGB,* in B. Von Heintschel-Heinegg (Hrsg), *Beck-Online Kommentar StGB,* XLVII ed., München, 2020, par. 15.

[471] EISELE J., *sub § 202d StGB,* cit., par. 25.

di cui alla lett. a) e la preparazione di cui alla lett. b) vi sia *concurso medial*, dato che quest'ultimo costituisce antecedente necessario per la frode informatica consumata[472]. Per quanto riguarda il concorso tra la frode informatica e i reati contro l'intimità personale, ovvero i reati di cui all'art. 197 c.p., si ritiene vi sia concorso di reati e non concorso apparente di norme, dato che i beni giuridici tutelati sono diversi[473]. Nel caso in cui l'accesso abusivo sia finalizzato a commettere una frode informatica tra i due reati vi sarà *concurso medial*[474].

5. La falsificazione e l'indebito uso degli strumenti di pagamento diversi dal contante

Nell'ordinamento tedesco gli strumenti di pagamento diversi dal contante trovano specifica tutela ai §§ 152a, 152b e 266b dello *Strafgesetzbuch*, che sanzionano rispettivamente la falsificazione degli strumenti di pagamento e l'uso improprio delle carte di credito. Il §152a StGB sanziona la falsificazione di carte di pagamento, assegni e cambiali e altri strumenti di pagamento fisici diversi dai contanti ("*Fälschung von Zahlungskarten, Schecks, Wechseln und anderen körperlichen unbaren Zahlungsinstrumenten*")[475], mentre il § 152b StGB la falsificazione di carte di pagamento con funzione di garanzia (*Fälschung von Zahlungskarten mit Garantiefunktion*). Il primo reato fu inserito nello *Strafgesetzbuch* già con la 2. WiKG, mentre il secondo fu introdotto con la l. n. 65 del 27 dicembre 2003, di attuazione della direttiva 2001/413/CE relativa alle frodi e falsificazioni dei mezzi di pagamento diversi dai contanti. Le condotte sanzionate sono identiche, muta solo l'oggetto del reato. Infatti, oggetto del primo reato sono carte di pagamento, assegni, cambiali e altri strumenti di pagamento fisici diversi dai contanti, definiti dall'Abs. 4 come «*quelli appositamente protetti contro la contraffazione mediante progettazione o codifica*»[476]. Sono, dunque, le carte che sostituiscono un pagamento in contanti se utilizzate come previsto, ossia

[472] FARALDO CABANA P., *Las nuevas tecnologías*, cit., p. 117.
[473] AGUADO LÓPEZ S., ORTIZ NAVARRO J.F., CABEDO VILLAMÓN F., *Fraude elecrtónico. Su gestión penal y civil*, cit., p. 101 ss., p. 108.
[474] MUÑOZ CONDE F., *Derecho Penal. PE*, cit., p. 301.
[475] «*Wer zur Täuschung im Rechtsverkehr oder, um eine solche Täuschung zu ermöglichen, 1. inländische oder ausländische Zahlungskarten, Schecks, Wechsel oder andere körperliche unbare Zahlungsinstrumente nachmacht oder verfälscht oder 2. solche falschen Karten, Schecks, Wechsel oder anderen körperlichen unbaren Zahlungsinstrumente sich oder einem anderen verschafft, feilhält, einem anderen überlässt oder gebraucht, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft*» (Chiunque, per ingannare nel commercio legale o per consentire tale inganno, 1. contraffà o falsifica carte di pagamento nazionali o estere, assegni, cambiali o altri strumenti fisici di pagamento non in contanti, o 2. si procura, offre in vendita, consegna o utilizza tali carte, assegni, cambiali o altri strumenti fisici di pagamento non in contanti contraffatti per sé o per un'altra persona, è punito con una pena detentiva non superiore a cinque anni o con una pena pecuniaria).
[476] «*Zahlungskarten und andere körperliche unbare Zahlungsinstrumente im Sinne des Absatzes 1 sind nur solche, die durch Ausgestaltung oder Codierung besonders gegen Nachahmung gesichert sind*».

carte che consentono al titolare di trasferire denaro o un valore monetario[477]. Oggetto del §152b StGB, invece, sono le carte di pagamento con funzione di garanzia[478]. Si tratta, dunque, di ipotesi qualificata rispetto al §152a StGB, ma si applica quest'ultima norma nell'ipotesi in cui i suddetti mezzi di pagamento con funzione di garanzia non sono stati emessi da un istituto di credito o di servizi finanziari[479].

Come sopra accennato, le fattispecie sono state oggetto di modifiche a seguito della recente legge di attuazione della direttiva 713/2019/UE contro le frodi e le falsificazioni di pagamento di strumenti diversi dai contanti. In particolare, l'oggetto del reato di cui al §152a StGB è stato ampliato sino a ricomprendere tutti gli strumenti di pagamento diversi dai contanti che abbiano una loro fisicità, senza che sia necessario che lo strumento stesso abbia la forma di una carta di credito[480]. Il problema è che il legislatore tedesco ha deciso di dare attuazione solo all'art. 4 (Reati connessi all'utilizzazione fraudolenta di strumenti di pagamento materiali diversi dai contanti) della direttiva 713/2019/UE e non anche all'art. 5 (Reati connessi all'utilizzazione fraudolenta di strumenti di pagamento immateriali diversi dai contanti). Per cui ha specificato che l'oggetto del reato dev'essere uno strumento di pagamento materiale (*körperliche*). Dunque, le applicazioni meramente digitali, quali ad esempio le *App* di pagamento o le piattaforme virtuali, sono escluse dall'ambito di applicazione del reato in questione[481]. Infatti, il legislatore tedesco ha evidenziato che la condotta di ottenimento di uno strumento di pagamento immateriale diverso dai contanti di cui all'art. 5 della menzionata direttiva va incriminata solo se ha comportato la commissione di uno dei reati di cui agli articoli da 3 a 6 della direttiva 2013/40/UE, «*già sanzionati ai sensi dei §§ 202a ss. e 303a s. StGB*»[482]. Per quanto riguarda, invece, le ulteriori condotte

---

[477] WEIDEMANN M., *sub §152a StGB*, in B. von Heintschel-Heinegg (a cura di), *Beck-Online Kommentar Strafgesetzbuch*, VIII Ed., München, 2022, Rn. 4, disponibile *online* al sito https://beck-online.beck.de.

[478] La definizione di "funzione di garanzia" è fornita dallo stesso § 152b StGB, che specifica che sono carte di pagamento con funzione di garanzia quelle carte di credito, Eurocheque o altre nelle quali l'emittente fornisce la garanzia del pagamento nelle operazioni di pagamento e che per il loro *design* o codificazione (PIN) sono protette in modo particolare contro la contraffazione (*(4) Zahlungskarten mit Garantiefunktion im Sinne des Absatzes 1 sind Kreditkarten und sonstige Karten, 1. die es ermöglichen, den Aussteller im Zahlungsverkehr zu einer garantierten Zahlung zu* veranlassen*, und 2. durch Ausgestaltung oder Codierung besonders gegen Nachahmung gesichert sind*).

[479] WEIDEMANN M., *sub StGB § 152b*, in B. von Heintschel-Heinegg (a cura di), *Beck-Online Kommentar Strafgesetzbuch*, VIII Ed., München, 2022, Rn. 2, disponibile *online* al sito https://beck-online.beck.de.

[480] *Deutscher Bundestag Drucksache n. 19/25631 del 5 gennaio 2021, Gesetzentwurf der Bundesregierung zur Änderung des Strafgesetzbuches – Umsetzung der Richtlinie (EU) 2019/713 des Europäischen Parlaments und des Rates vom 17. April 2019 zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln und zur Ersetzung des Rahmenbeschlusses 2001/413/JI des Rates*, p. 21, disponibile *online* al sito https://www.bundestag.de/drucksachen.

[481] WEIDEMANN M., *sub §152a StGB*, cit., Rn. 5.

[482] *Deutscher Bundestag Drucksache n. 19/25631*, cit., p. 10, secondo cui: «*Die Richtlinie verlangt nicht, dass die entsprechende Erlangung eines Zahlungsinstruments über die Strafbarkeit gemäß den Artikeln 3 bis 6 der Richtlinie 20213/40/EU hinaus zusätzlich unter Strafe gestellt wird*» (La direttiva non richiede che

previste dalle lett. b), c) e d) dell'art. 5 cit., il legislatore tedesco ha ritenuto che le stesse fossero già sono punibili come alterazione di dati (§ 303a StGB), frode informatica (§ 263a StGB), preparazione di frode informatica (§ 263a Abs. 3 StGB) o falsificazione di dati rilevanti ai fini probatori (§ 269 StGB). Per quanto riguarda le condotte di detenzione e il possesso degli strumenti di pagamento diversi dai contanti ottenuti illecitamente, contraffatti o falsificati (art. 4 lett. c) e art. 5 lett. c) della direttiva 713/2019) il legislatore tedesco ha ritenuto le stesse già astrattamente punibili a titolo di riciclaggio (§261 StGB) o, comunque, di frode informatica (§263a Abs. 3 StGB) o ricettazione di dati (§202d StGB)[483], per cui ha deciso di non modificare ulteriormente le leggi penali vigenti. Anche l'oggetto del reato di cui al §152b StGB, è stato modificato, ma, al contrario, in questo caso il legislatore si è limitato ad eliminare gli *eurocheque* dagli oggetti del reato.

Beni giuridici protetti dal §152a StGB sono la sicurezza e la funzionalità dei mezzi di pagamento diversi dai contanti[484], come peraltro riconosciuto dalla stessa giurisprudenza[485]. Lo stesso vale per il §152b StGB[486]. Condotte sanzionate dalle due norme sono la copia e la falsificazione degli oggetti ivi indicati[487]. Tali condotte comprendono, in definitiva, tutte le modalità che portano alla creazione di una carta di pagamento contraffatta, di un assegno contraffatto, di una cambiale contraffatta o di uno strumento di pagamento fisico diverso dai contanti contraffatto, senza che vi sia necessariamente un modello autentico per l'oggetto del reato o che il presunto emittente sia realmente esistente[488]. Il risultato dell'atto di falsificazione deve quindi essere costituito da carte di pagamento false o altri strumenti fisici di pagamento non in contanti che non provengono dall'emittente autorizzato[489]. Elemento soggettivo richiesto è il dolo, comprensivo della tendenza interna dell'inganno nei negozi giuridici (*zur Täuschung*), che, però, non assurge a livello dell'*Absicht* o intenzione criminosa[490]. Se le carte di pagamento prodotte sono più di una, si

l'ottenimento di uno strumento di pagamento sia ulteriormente punibile oltre alla responsabilità penale prevista dagli articoli da 3 a 6 della direttiva 20213/40/UE).

[483] *Deutscher Bundestag Drucksache n. 19/25631*, cit., p. 18.

[484] PUPPE I., SCHUMANN K., *sub StGB § 152a*, in U. Kindhäuser, U. Neumann, U. Paeffgen (a cura di), *Strafgesetzbuch*, cit., Rn. 3.

[485] BGH, Urteil vom 21. 9. 2000 - 4 StR 284/00.

[486] WEIDEMANN M., *sub §152a StGB*, cit., Rn. 2.

[487] *Ibid*., Rn. 8.

[488] ERB V., *sub StGB § 152a*, in V. Erb, J. Schäfer (a cura di), *Münchener Kommentar zum Strafgesetzbuch*, cit., Rn. 9.

[489] BGH, sentenza 21 settembre 2000 - 4 StR 284/00.

[490] ERB V., *sub StGB § 152a*, cit., Rn. 12..

configura un unico reato solo se la produzione viene effettuata in un'unica operazione continua in stretta connessione spaziale e temporale[491].

Le fattispecie di cui ai §§ 152a e 152b StGB sanzionano anche il successivo utilizzo non autorizzato delle carte di credito clonate presso sportelli *bancomat* o presso terminali POS. In questo caso, a differenza di quanto avviene per il reato di cui all'art. 493-*ter* c.p., che costituisce una disposizione a più norme, si configura un unico reato[492]. Va però evidenziato che l'inserimento di una carta di credito clonata in un *bancomat* o comunque per pagare ad un terminale POS viene sanzionata anche quale *Computerbetrug*, in particolare secondo la modalità dell'utilizzo non autorizzato di dati (v. *supra* par. 4)[493]. In questo caso tra i due reati si configurerà unità di azione (*Tateinheit*), con l'applicazione della sola fattispecie più grave[494]. Se, invece, la carta non viene contraffatta, ma semplicemente rubata e poi inserita o comunque utilizzata in un terminale POS si configura unicamente la frode informatica[495]. Peraltro, giurisprudenza più recente ha invece escluso si configuri la frode informatica nel caso in cui il criminale informatico posizioni uno *skimmer* per la lettura e la memorizzazione dei dati dei clienti di un bancomat, evidenziando che non potrebbe configurarsi quell'interferenza nel procedimento di elaborazione dei dati vietata ai sensi del §263a StGB qualora da quest'ultima non derivi direttamente un danno patrimoniale[496]. Il danno patrimoniale richiesto dal § 263a StGB, infatti, deve essere la conseguenza diretta del trattamento di dati[497]. Ciò dimostra che, a differenza di quanto sostenuto dal legislatore tedesco in sede di attuazione della citata direttiva 713/2019/UE, non è affatto pacifico che le condotte di falsificazione di strumenti di pagamento immateriali rientrino *tout court* nell'ambito applicativo della frode informatica. Non sembra, dunque, che la normativa di attuazione sia rispettosa dei requisiti previsti dalla direttiva.

Oltre a tali paragrafi, anche il già menzionato §266b StGB[498] sanziona l'uso improprio di carte di credito. A differenza delle due disposizioni sopra menzionate,

---

[491] BGH, sentenza 10 maggio 2005 – 3 StR 425/04; BGH, ordinanza 11 agosto 2011 – 2 StR 91/11.
[492] BGH, ordinanza 20 dicembre 2012 - 4 StR 458/12; BGH, sentenza 10 maggio 2005 - 3 StR 425/04.
[493] KOCHHEIM D., *Cybercrime und Strafrecht*, cit., p. 202.
[494] BGH, ordinanza 20 dicembre 2012 - 4 StR 458/12; BGH, ordinanza 23 giugno 2010 – 2 StR 243/10.
[495] Ibid., p. 202.
[496] BGH, ordinanza 12 novembre 2015 − 2 StR 197/15.
[497] BGH, ordinanza 22 gennaio 2013 – 1 StR 416/12. In tal senso v. anche HEFENDEHL R., NOLL M., *sub StGB § 263a Computerbetrug*, in V. Erb, J. Schäfer (a cura di), *Münchener Kommentar zum Strafgesetzbuch*, V ed. München, 2022, Rn. 179.
[498] «*Wer die ihm durch die Überlassung einer Scheckkarte oder einer Kreditkarte eingeräumte Möglichkeit, den Aussteller zu einer Zahlung zu veranlassen, mißbraucht und diesen dadurch schädigt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft*» (Chiunque abusi della possibilità offertagli dalla fornitura di una carta assegno o di una carta di credito per indurre l'emittente a effettuare un pagamento, danneggiando così l'emittente, è punito con la pena detentiva non superiore a tre anni o con la pena pecuniaria).

quest'ultima non richiede la falsificazione della carta di credito. Il §266b fu introdotto nello *Strafgesetzbuch* già dal 2.WiKG. ed il bene giuridico tutelato è il patrimonio dell'emittente della carta di credito o dell'assegno, come peraltro risulta chiaramente dalla formulazione della norma («*danneggiando così l'emittente*»), mentre l'interesse pubblico al corretto funzionamento del sistema di pagamento è tutelato solo in via riflessa[499]. Già da questo si evince la differenza tra questa fattispecie e il sopra esaminato art. 493-*ter* c.p., che tutela in via primaria un interesse pubblico. Al contrario di quanto avviene in Italia, quest'ultima fattispecie è sanzionata in modo più lieve rispetto alla *Computerbetrug*. Oggetto del reato sono esclusivamente le carte assegno (*bancomat* e in passato carta Eurocheque) e le carte di credito con obbligo di garanzia dell'emittente della carta nei confronti di terzi[500]. Dunque, non è applicabile in caso di utilizzo del mero codice alfanumerico o comunque della sola striscia magnetica della carta[501]. Condotta sanzionata è l'abuso dello strumento di pagamento, requisito da determinarsi esclusivamente con riferimento al rapporto contrattuale sottostante tra l'emittente della carta e il titolare della stessa[502], che deve aver danneggiato il patrimonio dell'emittente della carta. A tal proposito, è però controverso se vi debba essere un danno effettivo o se sia sufficiente un pericolo di danno[503]. Trattasi di reato proprio, che può essere commesso solo dai titolari dell'assegno o della carta di credito che sono autorizzati rispetto all'emittente e da coloro che hanno ottenuto il rilascio della carta fornendo informazioni false sulla propria persona e sulla propria situazione finanziaria[504]. Dunque, nel caso in cui le disposizioni siano effettuate da persona diversa dal titolare della carta, la responsabilità penale per indebito utilizzo della stessa ad un terminale POS è configurabile unicamente ai sensi del § 263a StGB[505]. È stato osservato che i sistemi di pagamento diversi dai contanti attualmente in uso si sono comunque allontanati di fatto dai sistemi di pagamento che il legislatore conosceva quando la disposizione in questione è stata introdotta nel 1988, così come il quadro giuridico di riferimento, per cui la fattispecie in questione necessiterebbe di un aggiornamento[506]. Tuttavia, tale norma non è stata oggetto di alcuna modifica in sede di recepimento della menzionata direttiva 2019/713/UE ed è rimasta

[499] RADTKE H., *StGB § 266b*, in V. Erb, J. Schäfer (a cura di), *Münchener Kommentar zum Strafgesetzbuch*, cit., Rn. 1.
[500] WITTIG P., *sub StGB § 266b*, in B. von Heintschel-Heinegg (a cura di), *Beck Online Kommentar Strafgesetzbuch*, Rn. 7 e 12.
[501] YOO Y.B., *Codekartenmißbrauchen am POS-Kassen-System. Strafrechtliche Überlegungen zur Computerkriminalität*, Frankfurt am Main, 1997, p. 119.
[502] WITTIG P., sub StGB § 266b, cit., Rn. 16.
[503] RADTKE H., *StGB § 266b*, cit. 71.
[504] WITTIG P., sub StGB § 266b, cit., Rn. 6
[505] HEGER E., *sub StGB § 266b*, in K. Lackner, K. Kühl, *Strafgesetzbuch*, XXIX ed., München, 2018, Rn. 2.
[506] RADTKE H., *StGB § 266b*, cit., Rn. 3.

immutata. È evidente che la fattispecie in questione è ormai obsoleta e non appare idonea a sanzionare i nuovi fenomeni criminosi sopra descritti e rischia di essere di fatto abrogata. Grossa limitazione, peraltro, è data dal fatto che la stessa tutela interessi patrimoniali della Banca, non un interesse pubblico quale ad esempio la tutela della pubblica fede. L'obsolescenza caratterizza però anche le norme di cui ai §§ 152a e 152b StGB, poiché sempre più spesso i nuovi strumenti di pagamento sono immateriali. Peraltro, come si è sopra esaminato, vi sono resistenze da parte della giurisprudenza tedesca a far rientrare *tout court* la falsificazione di strumenti di pagamento diversi dai contanti nell'ambito applicativo della *Computerbetrug* e ciò rischia di creare pericolosi vuoti di tutela. È certamente vero che a seguito della modifica dell'Abs. 3 del §263a StGB molti comportamenti criminosi di questo tipo possono rientrare nell'ambito applicativo degli atti preparatori alla commissione di truffa mediante computer, ma va ricordato che quest'ultima non ha la sanzione penale idonea richiesta dalla direttiva. Si ritiene opportuno, dunque, un ripensamento da parte del legislatore tedesco.

Anche nell'ordinamento spagnolo la falsificazione degli strumenti di pagamento costituisce reato a sé stante di cui all'art. 399-*bis* c.p. Tale norma, introdotta dalla *Ley Orgánica* 5/2010 per risolvere i problemi in merito all'applicabilità della fattispecie di falsificazione di moneta alle carte di credito[507] e recentemente modificata dalla *Ley Orgánica* 14/2022, si divide in quattro commi. Trattandosi di un reato di falso, si può ritenere che anche in questo caso bene giuridico tutelato sia la sicurezza del traffico giuridico o la pubblica fede[508]. Oggetto del reato in questione, per tutti i quattro commi, sono carte di credito o di debito o *travel cheques* e, a seguito della *Ley Orgánica* 14/2022, anche qualsiasi strumento di pagamento diverso dai contanti. Quest'ultimo viene definito dal successivo art. 399-*ter* c.p. come qualsiasi dispositivo, oggetto o registro protetto, materiale o immateriale, o una loro combinazione, diverso dalla moneta a corso legale, che, da solo o in combinazione con un processo o un insieme di processi, consenta al detentore o all'utente di trasferire denaro o valore monetario, anche attraverso mezzi di scambio digitali. Analogamente al legislatore italiano, dunque, il legislatore spagnolo ha dato attuazione sia all'art. 4 che all'art. 5 della direttiva 2019/713/UE. Anche in questo caso, come in Italia e Germania, non sono

[507] FARALDO CABANA P., *Las nuevas tecnologías*, cit., p. 273 ss.
[508] BACIGALUPO ZAPATER E., *Falsedad documental, estafa*, cit., p. 13.

ricomprese le le c.d. carte fedeltà o carte acquisti[509]. A seguito della modifica legislativa, però, si può ritenere che la norma tuteli anche le carte prepagate.

Trattasi di reato comune, ma la pena può variare a seconda del fatto che il soggetto abbia partecipato o meno alla falsificazione[510]. Al primo comma si sanziona colui che altera, copi, riproduca o falsifichi in qualsiasi modo una carta di credito, debito, *travel cheques* o qualsiasi altro strumento di pagamento diverso dai contanti. Per alterazione si intende la manipolazione effettuata su alcuni componenti della carta di credito (ad es. la banda magnetica), mentre per copia e riproduzione la clonazione o duplicazione dei dati ivi contenuti[511]. Le condotte descritte, dunque, si riferiscono tutte al dare un'apparenza di autenticità alle carte di credito mediante la clonazione visibile all'esterno o comunque dei loro numeri o dei dispositivi di identificazione correlati[512]. La giurisprudenza ha specificato che costituisce falsificazione anche la costruzione di una carta di credito su un supporto plastificato utilizzando i dati di una carta di credito previamente copiati e aggiungendo i dati personali di una persona diversa dal legittimo titolare dei dati della carta clonata[513]. Dunque, nell'ambito applicativo della norma in questione rientra lo *skimming*, nonché l'utilizzo dei numeri di carte di credito e PIN illecitamente carpiti per creare carte di credito false[514]. Per la consumazione di tale reato non è necessario che vi sia l'effettiva utilizzazione della carta di credito clonata[515]. Tuttavia, poiché il reato in questione si consuma con la clonazione, esso rimane allo stadio del tentativo nel caso in cui il reo abbia solo copiato i numeri delle carte e installato una telecamera per poter scoprire i PIN degli utenti[516].

Per quanto riguarda l'elemento soggettivo, vi è chi ritiene che sia necessaria la volontà di arrecare un pregiudizio patrimoniale al titolare o ad un terzo, mentre la cessione volontaria di tali oggetti sarebbe non punibile[517]. Tale requisito, però, non è specificato nella norma in questione.

La giurisprudenza considera come autore del reato in questione, o quantomeno responsabile a titolo di cooperazione necessaria, non solo chi materialmente confeziona la

[509] GÓMEZ MARTÍN V., *De la falsificación de tarjetas de crédito y débito y cheques de viaje*, in M. Corcoy Bidasolo, S. Mir Puig (a cura di), *Comentario al Código Penal. Reforma LO 5/2010*, Valencia, 2011, p. 871 ss., p. 872.
[510] MORÓN LERMA E., *Art. 399-bis*, in G. Quintero Olivares (dir.), F. Morales Prats (coord.), *Comentarios a la parte especial del derecho penal*, cit., p. 1616 ss., p. 1619 s.
[511] *Ibid*.
[512] FLORES PRADA I., *Criminalidad informática*, cit., p. 232.
[513] Tribunal Supremo, sez. I penale, sentenza 4 novembre 2016, n. 836.
[514] MORÓN LERMA E., *Art. 399-bis*, cit., p. 1620.
[515] Tribunal Supremo, sez. I penale, sentenza 12 maggio 2015, n. 267.
[516] Tribunal Supremo, sez. I penale, sentenza 19 novembre 2014, n. 771.
[517] FLORES PRADA I., *Criminalidad informática*, cit., p. 232.

carta falsificata, ma anche colui che fornisce i propri dati personali o documenti di identità in modo che possano essere utilizzati dalla persona stessa che li fornisce[518]. In relazione al 399-*bis*.1 c.p. è prevista una circostanza aggravante speciale qualora gli oggetti contraffatti rechino pregiudizio ad una pluralità di persone o quando i fatti siano commessi da appartenenti ad organizzazioni criminali dedite a tali attività. Anche in questo caso, per quanto riguarda il concetto di organizzazioni criminali, si deve fare riferimento all'art. 570-*bis*.2 c.p.[519].

All'art. 399-*bis*.2 si sanziona la detenzione di tali oggetti con la stessa pena prevista per la falsificazione. Tuttavia, a differenza dell'art. 493-*ter* c.p. italiano, la detenzione non è sanzionata per se stessa, ma soltanto se finalizzata alla successiva distribuzione o al commercio[520]. Trattasi, pertanto, di condotta preparatoria rispetto alla successiva distribuzione[521]. A seguito della *Ley Orgánica* 14/2022 è stato introdotto un nuovo art. 399 *bis*.4 c.p., che punisce la detenzione di tali strumenti finalizzata al loro utilizzo con pena più mite. La differenza tra le due ipotesi di reato, dunque, risiede nell'intenzione criminosa dell'agente. Si evidenzia, però, che non in tutti i casi appare facile distinguere tra le due ipotesi. A tutt'oggi, dunque, la mera detenzione di tali oggetti è ancora non punibile, poiché in entrambi i casi vi è la richiesta di una finalità[522].

Infine, vi è l'art. 399-*bis*.3, che sanziona la condotta di colui che, seppur non intervenuto nella falsificazione, sia consapevole della falsificazione della carta stessa e la utilizzi in pregiudizio di un'altra persona[523]. Con tale norma, dunque, si è voluto creare un regime speciale per coloro che, pur non avendo concorso nella falsità, utilizzino comunque la carta di credito falsificata. Per cui, secondo alcuni, si tratterebbe di un'ipotesi aggravata di frode[524]. In questo caso la pena prevista è minore rispetto alla falsificazione di cui al par. 1, ma non della frode informatica.

Nell'ordinamento spagnolo, al contrario di quello tedesco e italiano, l'indebito uso di carte di credito viene considerato come *estafa* e ivi sanzionato dal sopra esaminato art. 249.1 lett. b) c.p. Inoltre, a seguito della *Ley Orgánica* 14/2022 il nuovo art. 249.3 c.p.

---

[518] Tribunal Supremo, sez. I penale, sentenza 4 novembre 2016, n. 836; Tribunal Supremo, sez. I penale, sentenza 12 maggio 2015 n. 267.
[519] GÓMEZ MARTÍN V., *De la falsificación de tarjetas de crédito y débito*, cit., p. 875.
[520] Tribunal Supremo, sez. I penale, sentenza 9 febbraio 2015, n. 68.
[521] MORÓN LERMA E., *Art. 399-bis*, cit., p. 876.
[522] FLORES PRADA I., *Criminalidad informática*, cit., p. 233.
[523] «*El que sin haber intervenido en la falsificación usare, en perjuicio de otro y a sabiendas de la falsedad, tarjetas de crédito o débito, cheques de viaje o cualesquiera otros instrumentos de pago distintos del efectivo falsificados, será castigado con la pena de prisión de dos a cinco años*».
[524] MORÓN LERMA E., *Art. 399-bis*, cit., p. 1623.

sanziona anche le condotte del possesso, acquisizione, trasferimento, distribuzione o messa a disposizione di terzi di carte di credito o debito, *travel cheques* e qualsiasi altro mezzo di pagamento materiale o immateriale diverso dai contanti, se commesse al fine di fare un uso fraudolento di tali strumenti[525].

Per quanto riguarda il *carding*, la giurisprudenza spagnola lo qualifica unicamente come *estafa informática* ex art. 248.2. lett. c) (oggi 249.1 lett. b) e non come falsificazione di carta di credito ex art. 399-*bis* c.p., posto che i criminali si limitano unicamente ad utilizzare i numeri autentici e genuini della carta di credito ottenuti con la tecnica del *phishing* o dello *skimming*[526].

Per quanto riguarda il rapporto tra la falsificazione della carta di credito e il suo successivo indebito utilizzo, il *Tribunal supremo* ha ritenuto vi sia *concurso medial* di cui all'art. 77 *código penal* tra il reato continuato di cui all'art. 399-*bis* c.p. e l'*estafa* ex art. 248.2 lett. c) (oggi 249.1 lett b) c.p., dato che la falsificazione costituisce il reato-mezzo per realizzarne l'indebita utilizzazione[527]. Dunque vi è concorso di reati e non concorso apparente di norme. A tal proposito, si evidenzia che la pena prevista per la contraffazione non assorbe il disvalore giuridico derivante dal successivo utilizzo indebito della carta e che i due reati sono posti a tutela di beni giuridici diversi, per cui nel caso in cui il reo falsifichi la carta e poi la utilizzi sarà chiamato a rispondere di entrambi i reati.

Diversamente, per quanto riguarda i rapporti tra l'ipotesi di cui all'art. 399 *bis*.3 e l'art. 248.2 (oggi 249) c.p., la giurisprudenza del *Tribunal supremo* ritiene che le stesse siano tra loro in rapporto di *alternatividad*, dato che la prima è in rado di assorbire integralmente il disvalore dell'ultima, per cui si tratta di un'ipotesi di concorso apparente di norme[528].

[525] «*Se impondrá la pena en su mitad inferior a los que, para su utilización fraudulenta y sabiendo que fueron obtenidos ilícitamente, posean, adquieran, transfieran, distribuyan o pongan a disposición de terceros tarjetas de crédito o débito, cheques de viaje o cualesquiera otros instrumentos de pago materiales o inmateriales distintos del efectivo*».

[526] Sala de Apelación de la Audiencia Nacional, Madrid, sez. LXIV penale, sentenza 28 giugno 2022, n.7.

[527] Tribunal Supremo, sez. I penale, sentenza 29 ottobre 2019, n. 515; Tribunal Supremo, sez. I penale, sentenza 23 aprile 2014, n. 330; Tribunal Supremo, sez. I penale, sentenza 17 giugno 2013, n. 560.

[528] Tribunal Supremo, sez. I penale, sentenza 23 aprile 2014, n. 330; Tribunal Supremo, sez. I penale, sentenza 17 giugno 2013, n. 560.

6. I reati contro la disponibilità, l'integrità e la funzionalità dei dati e dei sistemi informatici

Nello *Strafgesetzbuch* la protezione dei dati rispetto alle modifiche non autorizzate e alla loro distruzione è affidata al § 303a StGB che punisce l'alterazione dei dati (*Datenveränderung*) e al § 303b StGB che sanziona il sabotaggio informatico (*Computersabotage*). Il legislatore tedesco, dunque, come quello italiano, distingue correttamente tra interferenza relativa ai dati e interferenza relativa ai sistemi, come prescritto dalla *Convenzione Cybercrime*. Queste fattispecie furono introdotte già dal 2.WiKG e collocate a fianco del danneggiamento tradizionale. Per questo motivo, i primi commentatori le classificarono tra gli *Eigentumsdelikte*[529]. Oggi, tuttavia, si riconosce che il bene giuridico tutelato da queste due norme non è unicamente il patrimonio, ma anche il diritto espressamente riconosciuto dalla *Bundesverfassungsgericht* all'integrità dei dati e sistemi informatici[530], nonché l'interesse della persona autorizzata a fruirne illimitatamente[531]. Tali norme furono poi oggetto di modifica a seguito della citata l. 11 agosto 2007 n. 1786, con la quale fu aggiunta la punibilità degli atti preparatori, nonché la circostanza aggravante del trattamento di dati di importanza essenziale di cui al §303b Abs. 2 StGB e le ulteriori circostanze aggravanti di cui al §303b Abs. 4 StGB, tra cui l'ipotesi del danno patrimoniale di rilevante entità e della compromissione della fornitura di beni o servizi essenziali.

Nell'ordinamento spagnolo il danneggiamento informatico fu previsto sin dall'introduzione del *Código penal* del 1995, dapprima come ipotesi aggravata di danneggiamento e poi, con le successive riforme, elevato al rango di autonoma fattispecie. Con l'introduzione dell'art. 264 c.p., dunque, si risolse la disputa dottrinaria in merito all'applicabilità del danneggiamento tradizionale alla distruzione di dati informatici. Infatti, la peculiarità dei reati di danneggiamento previsti nel codice penale spagnolo è che essi richiedono in modo esplicito solo eccezionalmente che l'oggetto del reato sia una cosa materiale, per cui in tutti gli altri casi rileva esclusivamente che sia stato danneggiato un qualcosa che può essere oggetto di proprietà ed economicamente valutabile[532]. Per questo

[529] HAFT F., *Das Zweite Gesetz*, cit., p. 10.
[530] MARBERTH-KUBICKI A., *Computer- und Internetstrafrecht*, cit., p. 64.
[531] HILGENDORF E., VALERIUS B., *Computer- und Internetstrafrecht*, cit., p. 176 e 179.
[532] GONZÁLES RUS J.J., *Aproximación al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos*, in *RFDUCM*, n. speciale 12, 1982, p.107 ss., p. 140. Secondo SERRANO BUTRAGUEÑO I., *Los delitos de daños*, Pamplona, 1994, p. 73, invece, il danneggiamento di dati informatici poteva comunque essere sanzionato ai sensi del danneggiamento tradizionale, poiché i dati, potendo essere percepibili alla vista e raccolti, possiedono caratteristiche che li rendono idonei ad essere "oggetti materiali".

motivo, vi erano autori che ritenevano che il c.d. sabotaggio di dati fosse già ricompreso nell'ambito applicativo del danneggiamento tradizionale[533].

Con la riforma di cui alla *Ley Orgánica* 5/2010 cit., il reato di *daño informático* è stato trasferito all'art. 264 c.p., dunque è stato elevato al rango di fattispecie autonoma. Con la *Ley Orgánica* 1/2015 cit. di attuazione della direttiva 2013/40/UE sono state poi inserite anche la fattispecie di cui all'art. 264 bis *código penal*, che sanziona l'ostacolo o l'interruzione di un sistema informatico altrui. Come si è evidenziato, a differenza di quanto avviene nell'ordinamento tedesco e similmente a quello italiano, gli atti preparatori al danneggiamento informatico sono sanzionati in modo autonomo dall'art. 264-*ter* c.p. (v. *supra* par. 2). Data la loro collocazione sistematica, si ritiene che bene giuridico tutelato dalle norme in questione sia il patrimonio[534].

6.1. L'interferenza nei confronti dei dati

Per quanto riguarda l'ordinamento tedesco, il delitto di cui al § 303a StGB sanziona colui che cancella, sopprime, rende inutilizzabili e manomette i dati[535]. Con la cancellazione si richiede che i dati della specifica memoria siano resi irriconoscibili in modo tale da essere irrimediabilmente persi e non ricostruibili[536]. La soppressione dei dati avviene quando i dati sono temporaneamente o permanentemente sottratti all'accesso della persona autorizzata, che non può quindi più utilizzarli[537]. Rendere inutilizzabili, invece, significa compromettere in modo tale da non consentire più l'utilizzo per lo scopo previsto[538]. Infine, per manomissione dei dati si intende qualsiasi modifica del loro contenuto, compresa l'aggiunta di dati parziali[539]. Trattasi, dunque, analogamente a quanto avviene per i reati di danneggiamento informatico previsti nell'ordinamento italiano, di modalità che si

---

[533] GONZÁLES RUS J.J., *Protección penal de sistemas*, cit., p. 4; ROMEO CASABONA C.M., *Poder informático*, cit., p. 176 s.

[534] GALÁN MUÑOZ A., *Los ciberdelitos*, cit., p. 169. Non mancano però opinioni di segno contrario, v. ANDRÉS DOMÍNGUEZ A. C., *Reformas en daños*, cit., p. 549, secondo cui il legislatore spagnolo avrebbe dovuto collocare le norme in una sezione indipendente del codice, per marcare la differenza tra esse e i danneggiamenti tradizionali.

[535] «*Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft*» (Chiunque illegittimamente cancelli, sopprima, renda inutilizzabili o manometta i dati (§ 202a Abs. 2) è punito con la pena detentiva non superiore a due anni o con la pena pecuniaria).

[536] WEIDEMANN M., *sub StGB § 303a*, in B. Von Heintschel-Heinegg (Hrsg), *Beck-Online Kommentar StGB*, cit., Rn. 8.

[537] *Ibid*., Rn. 10.

[538] *Ibid*., Rn. 12.

[539] ZACZYK R., *sub StGB § 303a*, in U. Kindhäuser, U. Neumann, U. Paeffgen (a cura di), *Strafgesetzbuch*, cit., Rn. 10.

sovrappongono e non consentono una delimitazione esatta[540]. Secondo alcuni non sarebbero punibili le menomazioni a cui si può porre rimedio senza grandi sforzi, tempo e costi, poiché non supererebbero la soglia di punibilità prevista dalla norma[541].

Oggetto del reato di cui al §303a StGB sono i dati di cui al § 202a Abs. 2 StGB, che, dunque vengono tutelati a prescindere dal loro contenuto, dal loro valore patrimoniale o dalla loro natura segreta[542]. Anche se la norma non lo richiede espressamente, si ritiene che i dati di cui alla norma debbano essere necessariamente altrui[543]. Nella fattispecie, infatti, è presente una clausola di antigiuridicità speciale, perché si prevede che il reo debba agire "illegittimamente", che altrimenti sarebbe priva di significato. Elemento soggettivo, invece, è il dolo, che può essere anche generico e che deve estendersi a tutti gli elementi del reato, in particolare all'esistenza di un potere altrui e alla mancanza di un proprio potere di disposizione[544].

La dottrina si è interrogata in merito alla possibilità di ricondurre il fenomeno del *phishing* al delitto di cui al § 303a StGB, in particolare con riferimento alla condotta di "alterazione/modifica" dei dati[545]. Si è infatti evidenziato che quando il *phisher* invia una *e-mail* fraudolenta, questa viene prima temporaneamente archiviata sul server del provider della posta elettronica e poi archiviata nella posta del destinatario e si è discusso se questo procedimento potesse costituire "manomissione" ai sensi della suddetta norma. Tuttavia, si evidenzia che l'invio di una semplice *mail* di per sé comporta soltanto l'aumento dei dati contenuti nella casella della posta elettronica non una modifica in senso proprio, motivo per cui si esclude che il § 303a StGB sanzioni il *deceptive phishing*[546]. Vi è chi, invece, ritiene tale norma applicabile al fenomeno del *pharming*, poiché la modifica del *browser* del computer della vittima costituirebbe proprio quell'illegittima manomissione, da intendersi come riprogrammazione non autorizzata, vietata dalla disposizione in questione[547]. Si ritiene, poi, che la norma sanzioni anche lo *spamming*, qualora l'invio massiccio delle *e-mail* provochi un sovraccarico del sistema[548]. Nell'ambito applicativo di tale fattispecie rientra poi l'installazione di *malware* quali *keylogger*, *spylogger*, *plug-in* del *browser*, ecc.

---

[540] WEIDEMANN M., *sub StGB § 303a*, cit., Rn. 7. In tal senso anche p. 176.
[541] GERCHE M., BRUNST P.W., *Praxishandbuch Internetstrafrecht*, cit., p. 80.
[542] HILGENDORF E., VALERIUS B., *Computer- und Internetstrafrecht*, cit., p. 176.
[543] GERCHE M., BRUNST P.W., *Praxishandbuch Internetstrafrecht*, cit., p. 79. HILGENDORF E., VALERIUS B., *Computer- und Internetstrafrecht*, cit., p. 176.
[544] WEIDEMANN M., *sub StGB § 303a*, cit., Rn. 16.
[545] HANSEN D., *Strafbarkeit des Phishing*, cit., p. 104.
[546] *Ibid*.
[547] BORGES G., SCHWENK J., STUCKENBERG C., WEGENER C., *Identitätsdiebstahl*, cit., p. 234; POPP A., "*Phishing", "Pharming" und das Strafrecht*, cit., p. 86.
[548] MARBERTH-KUBICKI A., *Computer- und Internetstrafrecht*, cit., p. 75.

all'insaputa dell'utente, trattandosi di manomissione illegittima, poiché il *software* della vittima viene modificato a sua insaputa in modo che registri tutto quanto viene digitato sulla tastiera[549]. Infine, tale norma sanziona anche gli attacchi *denial-of-service*, nella misura in cui si verifica una perdita di dati[550].

Si è posto poi il problema dell'applicabilità del reato in questione nell'ipotesi in cui l'utente scarichi volontariamente il *malware* sul suo PC credendolo un *software* legittimo. In linea di principio, infatti, il consenso dell'avente diritto esclude l'antigiuridicità del fatto e, di conseguenza, il reato in questione[551]. Mentre la giustificazione del consenso basato sull'inganno è considerata irrilevante, il consenso ottenuto con l'inganno è ancora ampiamente considerato efficace perché dipende esclusivamente dalla sua esistenza fattuale, che ovviamente dipende dal significato e dallo scopo del reato. Di conseguenza, seguendo questa impostazione il consenso all'installazione di un componente aggiuntivo escluderebbe il reato, anche se il consenso è stato dato solo perché la parte che ha acconsentito non sapeva quali cambiamenti (negativi) avrebbe effettivamente portato il componente aggiuntivo. La questione, dunque, rimane estremamente dibattuta[552].

Come sopra menzionato, nell'ordinamento spagnolo, norma analoga al § 303a è costituita dall'art. 264 del *código penal*, che sanziona il danneggiamento informatico[553]. La norma punisce colui che cancella, danneggia, deteriora, altera, sopprime o rende inaccessibili dati informatici, programmi informatici o documenti informatici altrui. Per cancellare si intende far sparire con qualsiasi mezzo, per danneggiare compromettere, pregiudicare o rendere inutilizzabile, per alterare modificare in tutto in parte il contenuto, per sopprimere eliminare e per rendere inaccessibile impedire l'accesso, la consultazione o la disponibilità[554]. Si tratta di risultati alternativi tra loro[555], equivalenti dal punto di vista del disvalore penale[556]. L'utilizzo della clausola di apertura "in qualsiasi modo" evidenzia la

[549] BORGES G., SCHWENK J., STUCKENBERG C., WEGENER C., *Identitätsdiebstahl*, cit., p. 242.
[550] HILGENDORF E., VALERIUS B., *Computer- und Internetstrafrecht*, cit., p. 177; MARBERTH-KUBICKI A., *Computer- und Internetstrafrecht*, cit., p. 77.
[551] ZACZYK R., *sub StGB § 303a*, cit., Rn. 14.
[552] BORGES G., SCHWENK J., STUCKENBERG C., WEGENER C., *Identitätsdiebstahl*, cit., p. 243.
[553] «*El que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a tres años*».
[554] FLORES PRADA I., *Criminalidad informática*, cit., p. 176 s.
[555] GALÁN MUÑOZ A., *Los ciberdelitos*, cit., p. 173.
[556] ROMEO CASABONA C.M., *La penetración del derecho penal económico en el marco jurídico europeo*, in C. M. Romeo Casabona, F. Flores Mendoza (a cura di), *Nuevos instrumentos jurídicos en la lucha contra la delincuencia económica y tecnológica*, Granada, 2012, p. 331 ss., p. 368; GALÁN MUÑOZ A., *Los ciberdelitos*, cit., p. 173.

possibilità di commettere il danneggiamento in questione con qualsiasi tipologia di azione, sia diretta che remota, purché idonea a produrre il risultato in questione[557].

Oggetto materiale del reato in questione sono dati, documenti elettronici o programmi informatici, tutti quanti di persone estranee rispetto all'autore del reato[558]. Il requisito dell'altruità dei dati, presente anche nell'omologa fattispecie italiana, ma non in quella tedesca, è stato oggetto di critiche, perché finisce per limitare eccessivamente l'ambito applicativo della norma[559]. Si ritiene che la differenza tra dati e programmi informatici consista nel fatto che in questi ultimi i dati sono custoditi e ordinati in un supporto o sistema informatico. I dati, dunque, sono unità basiche di informazioni che una volta processati danno vita ad un'informazione, mentre i programmi informatici sono una sequenza di istruzioni o informazioni destinate ad essere utilizzate in un sistema informatico per eseguire una funzione o un compito o per ottenere un particolare risultato[560]. Il documento informatico, invece, viene inteso come insieme di istruzioni che, una volta eseguite in un sistema informatico, eseguono uno o più compiti[561].

Le condotte in questione devono causare un danno che sia economicamente valutabile[562]. Peculiarità di tale fattispecie rispetto al danneggiamento tradizionale, dunque, risiede nel fatto che per l'integrazione del reato in questione non è necessario che il danno sia riferito al supporto fisico nel quale i dati sono allocati, ma è sufficiente che riguardi il contenuto di quest'ultimo[563]. Anche in quest'ultimo caso l'azione non dev'essere non consentita o non autorizzata, requisito che viene inteso come azione compiuta senza la necessaria autorizzazione del proprietario o titolare di qualsiasi altro tipo di diritto sui dati[564].

Va evidenziato che, a differenza del legislatore italiano e di quello tedesco, il legislatore spagnolo ha preferito punire soltanto i casi che causino un risultato grave, possibilità riconosciuta dall'art. 3 della Decisione quadro 2005/222/GAI. La norma, però, non precisa quale sia il risultato grave, che risulta quindi un concetto giuridico indeterminato[565], foriero di problemi con riferimento al rispetto del principio di tassatività della norma penale, perché finisce per lasciare alla giurisprudenza il compito di definirne la

[557] DE LA MATA BARRANCO N. J., *Delitos contra los sistemas de información*, cit., p. 747.
[558] FERNÁNDEZ TERUELO J.G., *Derecho penal e* internet, cit., p. 98.
[559] SALVADORI I., *Los nuevos delitos informáticos*, cit., p. 240.
[560] DE LA MATA BARRANCO N. J., *Delitos contra los sistemas de información*, cit., p. 745.
[561] FERNÁNDEZ TERUELO J.G., *Derecho penal e* internet, cit., p. 98.
[562] FLORES PRADA I., *Criminalidad informática*, cit., p. 179; DE LA MATA BARRANCO N. J., *Delitos contra los sistemas de información*, cit., p. 750.
[563] FERNÁNDEZ TERUELO J.G., *Derecho penal e* internet, cit., p. 99.
[564] FLORES PRADA I., *Criminalidad informática*, cit., p. 175.
[565] GALÁN MUÑOZ A., *Los ciberdelitos*, cit., p. 172.

portata applicativa[566]. Per alcuni ciò significa che il legislatore richiede che il danno causato sia superiore alla soglia limite di 400 euro di cui al danneggiamento tradizionale ex art. 263[567]. Per altri, invece, si deve guardare al costo necessario per recuperare o ripristinare i dati o il sistema[568]. Per la dottrina maggioritaria il reato non sussiste qualora i dati archiviati possano essere recuperati o sia stata effettuata la copia di sicurezza[569]. Altri, invece, non reputano tale soluzione corretta e ritengono che anche in questo caso il reato sussista ugualmente, poiché si deve prendere come riferimento unicamente i costi di ripristino[570]. Altri ancora evidenziano che se si esclude la tipicità del fatto qualora i dati possano essere recuperati, si finisce per "punire" ingiustamente la vittima che in virtù del suo dovere di autoprotezione si è premurata di effettuare la copia dei dati rispetto a quella che non si è autoprotetta[571].

Il requisito della gravità del danno pone dei problemi con riferimento alle condotte di alterazione e inaccessibilità. Infatti, si discute se per l'integrazione del reato in questione queste ultime debbano essere definitive o possano essere anche temporanee. Alcuni autori escludono tale possibilità, evidenziando che difficilmente può ritenersi che i dati siano danneggiati nella loro sostanza o funzionalità se l'alterazione o l'inaccessibilità non è permanente[572]. Altri, invece, non ritengono adeguata tale soluzione e ritengono che la gravità del danno debba essere riferita esclusivamente al momento in cui il sistema viene alterato o reso indisponibile, non al fatto che lo stesso possa essere eventualmente ripristinato[573].

Per quanto riguarda l'elemento soggettivo, va evidenziato che peculiarità dell'ordinamento spagnolo è che, a differenza di Italia e Germania, i danneggiamenti possono essere sanzionati anche a titolo di colpa grave ai sensi dell'art. 267 c.p., purché il danno causato sia superiore ad 80.000 euro. Poiché, però, quest'ultima norma fa riferimento in via generale ai "danni", senza specificare anche quelli informatici, qualche autore si è

[566] SALVADORI I., *Los nuevos delitos informáticos,* cit., p. 239.
[567] ROMEO CASABONA C.M., *La penetración del derecho penal económico*, cit., p. 370; FLORES PRADA I., *Criminalidad informática*, cit., p. 180.
[568] FERNÁNDEZ TERUELO J.G., *Derecho penal e internet*, cit., p. 100.
[569] GONZÁLES RUS J.J., *Protección penal de sistemas*, cit. In tal censo in giurisprudenza v. Sección de Apelación Penal Madrid, V sez. penale, sentenza 23 ottobre 2015 n. 87, la quale ha escluso la sussistenza del danneggiamento informatico evidenziando che: «*Tal elemento típico valorativo normativo no ha quedado probado; desde el punto de vista del Hardware basta un nuevo disco duro para el restablecimiento del sistema informático*»
[570] FERNÁNDEZ TERUELO J.G., *Derecho penal e internet*, cit., p. 101.
[571] GALÁN MUÑOZ A., *Los ciberdelitos*, cit., p. 175.
[572] DE LA MATA BARRANCO N. J., *Delitos contra los sistemas de información*, cit., p. 749.
[573] GALÁN MUÑOZ A., *Los ciberdelitos,* cit., p. 175.

interrogato in merito alla punibilità dei danneggiamenti informatici a titolo di colpa[574]. La maggioranza degli autori ritiene che anche i danneggiamenti informatici siano puniti a titolo di colpa grave, sia per la collocazione sistematica dell'art. 267 c.p., sia perché il danno informatico costituisce comunque un danno[575]. Altri autori, tuttavia, sono contrari a tale conclusione e ritengono che il danneggiamento informatico dovrebbe essere punito unicamente a titolo doloso, evidenziando che lo stesso è in realtà un tipo autonomo o speciale rispetto al danneggiamento tradizionale e in nessuna delle normative europee si richiede la punibilità del danneggiamento a titolo colposo[576].

Anche in questo caso sono previste diverse ipotesi qualificate, ovvero l'aver commesso il fatto nell'ambito di un'organizzazione criminale, l'aver causato un danno di speciale gravità o che abbia riguardato un elevato numero di sistemi informatici, l'aver pregiudicato in modo grave il funzionamento di servizi pubblici essenziali o l'approvvigionamento di beni di prima necessità e, infine, l'aver causato un danno al sistema informatico di un'infrastruttura critica o aver creato una situazione di pericolo grave per la sicurezza dello Stato, dell'Unione europea o di uno Stato membro dell'Unione europea. All'art. 264.3 c.p. è prevista poi una circostanza aggravante per il fatto commesso attraverso l'uso illegittimo dei dati personali di un'altra persona per accedere al sistema informatico o per ottenere la fiducia di terzi. Tale circostanza, che richiama la previsione di cui all'art. 9 co. 5 della direttiva 2013/40/UE, è volta a punire più severamente il fatto commesso col c.d. furto o indebito utilizzo di identità digitale[577]. Tale disposizione, però, pone qualche problema con riferimento al concorso di reati, dato che, come sopra esaminato (v. *supra*, par. 3), nell'ordinamento spagnolo già esistono fattispecie volte a reprimere l'illecito trattamento di dati personali. In questo caso si ritiene si tratti di concorso apparente di norme da risolvere secondo il principio di *alternatividad*, con la sola applicazione dell'art. 264.3 c.p.[578].

Per quanto riguarda il rapporto tra le norme, si ritiene che il reato in questione possa concorrere coi reati contro la intimità di cui all'art. 197.1 e 2 c.p., data la diversità del bene

[574] TRAPERO BARREALES M. A., *¿Son punibles los daños informáticos imprudentes? Un debate (peligrosamente) abierto*, in *RECPC*, 2022, n. 24-18, p. 1 ss., p. 4.
[575] GALÁN MUÑOZ A., *Los ciberdelitos*, cit., p. 178; FERNÁNDEZ TERUELO J.G., *Derecho penal e Internet*, cit., p. 105; DE LA MATA BARRANCO N. J., *Delitos contra los sistemas de información*, cit., p. 742.; RODRIGUEZ MESA M.J., *Los delitos de daños. Capítulo IX del Título XIII del CP tras la reforma de la LO 1/2015*, Valencia, 2017, p. 115; ROMEO CASABONA C.M., *La penetración del derecho penal económico*, cit., p. 370.
[576] TRAPERO BARREALES M. A., *¿Son punibles los daños informáticos imprudentes?*, cit., p. 28.
[577] GALÁN MUÑOZ A., *Los ciberdelitos*, cit., p. 188.
[578] *Ibid*., p. 189.

giuridico tutelato[579]. Allo stesso modo, tale reato può concorrere con l'accesso abusivo a sistema informatico o telematico[580].

6.2. L'interferenza nei confronti dei sistemi informatici

Vanno ora esaminate le disposizioni in materia di interferenza illecita relativa ai sistemi, di cui all'art. 4 della direttiva 2013/40/UE e all'art. 5 della Convenzione *cybercrime*. Nell'ordinamento tedesco essa è sanzionata dal delitto di cui al § 303b StGB[581]. Tale norma punisce il disturbo significativo di un procedimento di elaborazione di dati (*Datenverarbeitung*) che avvenga con le modalità ivi indicate, ovvero secondo le modalità indicate nel §303a StGB (cancellare, sopprimere, rendere inutilizzabili e manomettere i dati), inserendo o trasmettendo dati con l'intenzione di arrecare un danno e distruggendo, danneggiando, rendendo inutilizzabile, rimuovendo o manipolando un sistema di elaborazione dati o un supporto dati[582]. Per disturbo si intende la compromissione del buon funzionamento in misura non trascurabile[583], che deve avvenire secondo le modalità indicate dalla norma. Dato il richiamo svolto dal §303b StGB alle condotte sanzionate dal §303a StGB, vi è chi ritiene che il legislatore tedesco dovrebbe unire le condotte sanzionate da entrambi i reati in uno unico, in modo da garantire un maggior coordinamento di sistema[584].

Le condotte di inserimento e trasmissione sono state aggiunte dalla l. 11 agosto 2007 n. 1786 cit., al fine di sanzionare i *Denial-of-service-attacks*[585]. Si è, quindi, voluto sanzionare le azioni di disturbo che derivano da modalità di condotta di per sé neutre, ma perpetrate con intenzioni lesive[586]. Per inserimento di dati si intende l'immissione di dati dall'esterno, che ha luogo prima della trasmissione e prima della loro memorizzazione[587]. A

---

[579] FERNÁNDEZ TERUELO J.G., *Derecho penal e Internet*, cit., p. 104. V. Anche Sentencia Juzgado de lo Penal n. 7 de Valencia 15 giugno 2004.
[580] FERNÁNDEZ TERUELO J.G., *Derecho penal e Internet*, cit., p. 104 s.
[581] «*Wer eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, dadurch erheblich stört, dass er 1. eine Tat nach § 303a Abs. 1 begeht, 2. Daten (§ 202a Abs. 2) in der Absicht, einem anderen Nachteil zuzufügen, eingibt oder übermittelt oder 3. eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft*» (Chiunque disturbi significativamente un procedimento di elaborazione di dati che sia per un altro indispensabile, mediante 1. la commissione di reato ai sensi del § 303a(1) StGB, 2. l'inserimento o trasmissione di dati (§ 202a Abs. 2) con l'intenzione di arrecare un danno a un'altra persona, oppure 3. distruggendo, danneggiando, rendendo inutilizzabile, rimuovendo o manomettendo un sistema di elaborazione dati o un supporto dati, è punito con la reclusione fino a tre anni o con la multa).
[582] MARBERTH-KUBICKI A., *Computer- und Internetstrafrecht*, cit., p. 82 ss.
[583] HILGENDORF E., VALERIUS B., *Computer- und Internetstrafrecht*, cit., p. 180.
[584] SIEBER U., *Straftaten und Strafverfolgung im Internet*, in *NJW-Beil*., 2012, p. 86 ss., p. 89.
[585] GRÖSELING N., HÖFINGER F.M., *Computersabotage und Vorfeldkriminalisierung. Auswirkungen des 41. StrÄndG zur Bekämpfung der Computerkriminalität*, in *MMR*, 2007, p. 626 ss., p. 626.
[586] MARBERTH-KUBICKI A., *Computer- und Internetstrafrecht*, cit., p. 83.
[587] WEIDEMANN M., *sub StGB § 303b*, in B. Von Heintschel-Heinegg (Hrsg), *Beck-Online Kommentar StGB*, cit., Rn. 12.

tal proposito, vi è chi ha criticato l'inserimento di questa nuova modalità di condotta, evidenziando l'impossibilità tecnica di "inserire" dati ai sensi del §202a StGB, poiché i dati possono essere inseriti attraverso un supporto esterno[588]. Per trasmissione, invece, si intende l'inoltro di dati da un computer all'altro all'interno di una rete esistente o tramite percorsi di telecomunicazione, il che dovrebbe includere anche la trasmissione tramite *W-LAN*[589]. Tale processo tecnico si completa a distanza e richiede una connessione di rete[590]. La differenza tra inserimento e trasmissione, dunque, consiste nel fatto che nel primo caso i dati vengono inviati direttamente al computer interessato e non come parte di un processo di inoltro[591].

Oggetto di tutela del § 303b StGB, invece, è un procedimento di elaborazione di dati, nozione che dev'essere intesa in senso lato, comprensiva anche del trattamento di dati[592], che però è tutelato solo se "indispensabile", ulteriore requisito richiesto dalla norma che evita la punibilità dei c.d. fatti bagatellari[593]. Il limite dell'"indispensabilità" viene superato solo se la funzionalità della rispettiva struttura dipende interamente o prevalentemente dallo svolgimento indisturbato dello specifico trattamento dei dati[594]. Dunque, il limite riguarda unicamente il trattamento dei dati, ai fini del superamento della soglia non sono determinanti la durata e l'intensità dell'attacco, ma solo l'importanza della stessa elaborazione dei dati disturbata[595]. Secondo la giurisprudenza è necessario esaminare caso per caso la presenza di questo requisito[596]. Si prescinde, dunque, dalle dimensioni del sistema informatico. Inoltre, a seguito della modifica legislativa del 2007 sono oggetto di tutela anche i sistemi informatici appartenenti a soggetti privati, non più unicamente quelli appartenenti ad aziende o imprese[597]. Ulteriore requisito è che il disturbo sia "significativo", escludendo in tal modo la semplice messa in pericolo[598]. A tal proposito, si è ritenuto che la menomazione non possa ritenersi "significativa" ai sensi della norma solo se il sistema può essere ripristinato senza un grosso dispendio di tempo e costi[599]. Dunque, non tutti i *Denial-of-Service-attacks* sono

[588] GRÖSELING N., HÖFINGER F.M., *Computersabotage und Vorfeldkriminalisierung*, cit., p. 627.
[589] WEIDEMANN M., *Sub StGB § 303b*, cit., Rn. 12.
[590] KOCHHEIM D., *Cybercrime und Strafrecht*, cit., p. 271.
[591] WEIDEMANN M., *Sub StGB § 303b*, cit., Rn. 12.
[592] GERCHE M., BRUNST P.W., *Praxishandbuch Internetstrafrecht*, cit., p. 82.
[593] WEIDEMANN M., *Sub StGB § 303b*, cit., Rn.; VALERIUS B., *Zur Strafbarkeit virtueller Sit-ins im Internet*, in E. Hilgendorf (a cura di), *Dimensionen des IT-Rechts*, Berlin, 2008, p. 19 ss., p. 38.
[594] HILGENDORF E., VALERIUS B., *Computer- und Internetstrafrecht*, cit., p. 180.
[595] VALERIUS B., *Zur Strafbarkeit virtueller Sit-ins im Internet*, cit., p. 39.
[596] BGH, sez. I penale, ordinanza 8 aprile 2021 – 1 StR 78/21.
[597] GERCHE M., BRUNST P.W., *Praxishandbuch Internetstrafrecht*, cit., p. 83.
[598] WEIDEMANN M., *Sub StGB § 303b*, cit., Rn. 15.
[599] MARBERTH-KUBICKI A., *Computer- und Internetstrafrecht*, cit., p. 82.

sanzionati dalla norma in questione[600], ma solo quelli che comportano una significativa menomazione.

Per quanto riguarda l'elemento soggettivo della fattispecie, il reato in questione è punito a titolo di dolo, che può essere anche eventuale[601]. Le condotte di cui all'Abs. 1 n. 2, però, richiedono che l'autore del reato agisca con il fine con l'intenzione di arrecare un danno. Tuttavia, lo stesso legislatore ha specificato che a tal fine è sufficiente la consapevolezza che il danno arrecato sia conseguenza necessaria dell'atto[602]. Inoltre, il concetto di svantaggio è inteso in senso ampio, per cui comprende qualsiasi menomazione, non necessariamente una perdita patrimoniale[603].

Nell'Abs. 2 è poi prevista un'ipotesi qualificata, per il caso in cui il procedimento di elaborazione sia di essenziale importanza per un'azienda o impresa altrui o per la pubblica amministrazione. Prima della riforma del 2007 quelle ivi indicate costituivano le ipotesi base del reato, la cui applicabilità, come si è evidenziato, è stata ora estesa anche ai sistemi informatici appartenenti a persone fisiche. In questo caso il trattamento dei dati è di importanza essenziale se il funzionamento dell'azienda nel suo complesso dipende interamente o prevalentemente dal suo funzionamento[604]. Infine, l'Abs. 4 prevede diverse ipotesi in cui il reato è da considerarsi aggravato, ovvero il caso in cui il reo cagioni in danno patrimoniale di rilevante entità, agisca professionalmente o come membro di un'associazione a delinquere istituita allo scopo di commettere sabotaggi informatici oppure qualora l'atto comprometta la fornitura di beni o servizi essenziali alla popolazione o la sicurezza dello Stato. Quest'ultima ipotesi, dunque, è destinata a trovare applicazione agli attacchi informatici diretti a danneggiare i *server* delle c.d. infrastrutture critiche, quali ad esempio gli ospedali.

Nell'ambito applicativo del *Computersabotage* rientrano non solo i *Denial-of-Service-attacks*, come pacificamente riconosciuto dalla giurisprudenza[605], ma anche l'installazione di *virus* e *worm*, non appena questi abbiano dispiegato il loro effetto dannoso[606], nonché lo *spamming*, qualora esso comprometta il sistema[607]. Non solo, ma vi

[600] HILGENDORF E., VALERIUS B., *Computer- und Internetstrafrecht*, cit., p. 181.
[601] WEIDEMANN M., *Sub StGB § 303b*, cit., Rn. 17.
[602] *Deutscher Bundestag Drucksache 16/3656. Gesetzentwurf der Bundesregierung Entwurf eines Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität (41. StrÄndG)*, p. 23, disponibile *online* all'indirizzo https://dipbt.bundestag.de/dip21/btd/16/036/1603656.pdf.
[603] VALERIUS B., *Zur Strafbarkeit virtueller Sit-ins im Internet*, cit., p. 39.
[604] WEIDEMANN M., *sub StGB § 303b*, cit., Rn. 23.
[605] V. LG Köln, sez XVIII penale, sentenza 28 luglio 2017 - 118 KLs 4/17; LG Düsseldorf, sentenza 22 marzo 2011 - 3 KLs 1/11.
[606] KOCHHEIM D., *Cybercrime und Strafrecht*, cit., p. 329.
[607] WEIDEMANN M., *sub StGB § 303b*, cit., Rn. 10.

rientra anche la distribuzione di un *malware* di tipo *ransomware*[608]. Si è, infatti, evidenziato che una volta che il *ransomware* è operativo, il blocco del *computer* o dei dati criptati può essere rimosso solo cancellando il disco rigido e reinstallando il sistema operativo, per cui all'infezione si associa una perdita irrevocabile di tutti i dati memorizzati. Inoltre, si è evidenziato che gli attacchi *ransomware*, interferendo con i file di registro dei sistemi informatici danneggiati, costituiscono alterazione di dati ai sensi del § 303 a, Abs. 1 StGB, dato che l'intero schermo e tutte le altre finestre vengono coperte dalla schermata di blocco e tutte le funzioni del sistema vengano interrotte dal *software* maligno[609]. Per quanto riguarda i rapporti con il reato di estorsione, la *Bundesgerichtshof* ha osservato che in caso di attacco *ransomware* si configura unità di azione (*Tateinheit*) tra i §§ 303b e 253 StGB, con applicazione della sola fattispecie punita più gravemente[610].

L'omologo spagnolo di cui al § 303b StGB è l'art. 264 *bis* del *código penal*. Tale norma fu introdotta dalla *Ley Orgánica* 1/2015 e sanziona l'ostacolo o l'interruzione del funzionamento del sistema informatico. Essa, tuttavia, riprende il contenuto del previgente art. 264.2 c.p. oggi sostituito, che sanzionava per l'appunto il sabotaggio informatico. Anch'essa, dunque, come l'omologo tedesco, richiama al suo interno le condotte già sanzionate dal danneggiamento informatico. Oggetto materiale del reato in questione è il sistema informatico, che viene inteso come unità informative digitali personali o professionali[611], anche se secondo alcuni è oggetto di tutela meramente strumentale rispetto ai dati informatici[612]. Anche in questo caso esso dev'essere "altrui", ovvero appartenente a persona diversa dall'autore. Quest'ultimo, inoltre, deve agire "senza essere stato autorizzato", disposizione che va intesa anch'essa come mancanza del consenso di chi può validamente disporne[613].

Tale norma prevede due eventi alternativi tra loro, ovvero l'ostacolo o l'interruzione di un sistema informatico, che devono realizzarsi mediante una delle condotte elencate dalla norma. Trattasi, pertanto, di fattispecie a forma vincolata[614]. Analogamente al § 303b StGB, la norma rinvia alle condotte descritte nel danneggiamento di dati e informazioni. Pertanto, qualora la cancellazione, il danneggiamento, il deterioramento, l'alterazione, la soppressione o l'inaccessibilità riguardino sistemi informatici, il danneggiamento informatico di cui

[608] BGH, ordinanza del 8 aprile 2021 – 1 StR 78/21, cit.
[609] *Ibid*.
[610] *Ibid*.
[611] FLORES PRADA I., *Criminalidad informática*, cit., p. 174.
[612] ROMEO CASABONA C.M., *La penetración del derecho penal económico*, cit., p. 369.
[613] DE LA MATA BARRANCO N. J., *Delitos contra los sistemas de información*, cit., p. 753.
[614] GALÁN MUÑOZ A., *Los ciberdelitos*, cit., p. 191.

all'art. 264 c.p. sarà assorbito nella fattispecie di cui all'art. 264 *bis* c.p.[615]. Ulteriori condotte previste sono quella dell'introduzione o trasmissione di dati, che possono produrre uno degli eventi tipici previsti dalla norma sia saturando il disco fisso del sistema informatico, sia sovraccaricando la rete di dati in modo tale che il sistema si sovraccarichi e non sia più in grado di operare[616]. L'ultima condotta, invece, consiste nel distruggere, danneggiare, rendere inutilizzabile, eliminare o sostituire un sistema informatico o telematico o di archiviazione elettronica delle informazioni. Diversamente dalle altre sopra menzionate, essa non era già prevista nel previgente art. 264.2 c.p., ma è stata introdotta ex novo dalla *Ley Orgánica* 1/2015 cit. e si è trattato di un'autonoma scelta da parte del legislatore spagnolo, dato che non si tratta di condotte elencate nell'art. 5 della direttiva 2013/40/UE[617]. La condotta in questione, comunque, riguarda l'*hardware* o i componenti fisici del sistema, non il *software*[618].

Poiché l'evento del reato in questione consiste nell'ostacolare o interrompere, non si pone la questione dell'irreversibilità o meno del danno, dato che è palese che l'interruzione può avere carattere meramente temporaneo[619]. Anche in questo caso è previsto il requisito della gravità del danno, gravità che, in questo caso, va riferita al pregiudizio patrimoniale causato, ovvero i costi sostenuti per il ripristino del sistema e il c.d. lucro cessante derivante dal mancato utilizzo del sistema[620].

Per quanto riguarda l'elemento soggettivo, in merito alla possibilità che lo stesso sia punito anche a titolo di colpa si rimanda a quanto già esposto per il reato di danneggiamento di dati, informazioni e programmi di cui all'art. 264 c.p. Anche in questo caso sono previste diverse ipotesi qualificate di reato, che sono le stesse già previste in materia di danneggiamento di dati, informazioni o programmi.

Nell'ambito applicativo della norma in questione rientrano tutte quelle condotte quali il *mail bombing* oppure l'installazione o trasmissione di *malware* che hanno quale effetto quello di interferire in modo grave sul corretto funzionamento del sistema informatico, nonché i *Denial-of-service-attacks*[621].

---

[615] *Ibid*.
[616] *Ibid*., p. 192.
[617] ANDRÉS DOMÍNGUEZ A.C., *Reformas en daños*, in *Comentario a la reforma penal de 2015*, cit., p. 539 ss., p. 547.
[618] GALÁN MUÑOZ A., *Los ciberdelitos*, cit., p. 192.
[619] DE LA MATA BARRANCO N. J., *Delitos contra los sistemas de información*, cit., p. 753.
[620] GALÁN MUÑOZ A., *Los ciberdelitos*, cit., p. 194.
[621] SALVADORI I., *Los nuevos delitos informáticos*, cit., p. 242.

Altra disposizione rilevante è quella di cui al § 317 StGB (*Störung von Telekommunikationsanlagen*)[622], che sanziona chiunque impedisca o metta in pericolo il funzionamento di un sistema di telecomunicazione che serve per scopi di pubblica utilità. La definizione di "sistema di telecomunicazione" è contenuta nel § 3 n. 60 della *Telekommunikationsgesetz* (TKG), ovvero «*apparecchiature o sistemi tecnici che trasmettono, commutano, ricevono, controllano o monitorano segnali elettromagnetici o ottici identificabili come messaggi*»[623]. Dunque, in tale nozione sono ricompresi gli impianti della rete pubblica di telecomunicazioni, che possono servire sia per la telefonia che per le comunicazioni via *Internet*, i quali sono così anche oggetto del reato del reato in questione[624]. Bene giuridico protetto dalla norma in questione è il buon funzionamento del sistema pubblico di telecomunicazioni[625]. Trattasi di reato di pericolo astratto che, ai sensi dell'Abs. 3, può essere punito anche a titolo di colpa[626]. Anche tale disposizione, unitamente ai §§ 303a e 303b StGB, sanziona gli attacchi *Distributed Denial of Service* qualora gli stessi siano diretti ad impianti di interesse pubblico. Infatti, la modalità di azione del "rendere inutilizzabile" richiede un impatto diretto, ma non fisico sul sistema, in modo che anche l'attacco tramite *malware* rientra nell'ambito applicativo della norma in questione[627]. Pure in questo caso si configurerà unità di azione[628].

Anche nell'ordinamento spagnolo vi è una norma apposita che sanziona il sabotaggio delle reti di telecomunicazione, ovvero l'art. 560 c.p.[629]. Trattasi di ipotesi qualificata del reato di danneggiamento, che si differenzia dalle ipotesi sopra elencate per via dell'oggetto del reato, ovvero "*líneas o instalaciones de telecomunicaciones*", tra cui sono ricomprese

---

[622] «*Wer den Betrieb einer öffentlichen Zwecken dienenden Telekommunikationsanlage dadurch verhindert oder gefährdet, daß er eine dem Betrieb dienende Sache zerstört, beschädigt, beseitigt, verändert oder unbrauchbar macht oder die für den Betrieb bestimmte elektrische Kraft entzieht, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft*» (Chiunque, impedisca o metta in pericolo il funzionamento di un impianto di telecomunicazione di pubblica utilità, distruggendo, danneggiando, rimuovendo, alterando o rendendo inutilizzabile una cosa al servizio del sistema o sottraendo l'energia elettrica ad esso destinata, è punito con una pena detentiva non superiore a cinque anni o con una sanzione pecuniaria).

[623] «*Technische Einrichtungen, Systeme oder Server, die als Nachrichten identifizierbare elektromagnetische oder optische Signale oder Daten im Rahmen der Erbringung eines Telekommunikationsdienstes senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können*».

[624] HILGENDORF E., VALERIUS B., *Computer- und Internetstrafrecht*, cit., p. 200.

[625] CORNELIUS K., *Sub 102 Besonderer Teil des Strafgesetzbuches*, in J. Taeger, J. Pohle (a cura di), *Computerrechts-Handbuch. Informationstechnologie in der Rechts-und Wirtschaftpraxis*, München, 2021, Rn. 206.

[626] GERCHE M., BRUNST P.W., *Praxishandbuch Internetstrafrecht*, cit., p. 86 s.

[627] HILGENDORF E., VALERIUS B., *Computer- und Internetstrafrecht*, cit., p. 201.

[628] ZIESCHANG F., *StGB sub § 317*, in U. Kindhäuser, U. Neumann, U. Paeffgen (a cura di), *Strafgesetzbuch. III Band*, V ed., Baden-Baden, 2017, Rn. 17.

[629] «*Los que causaren daños que interrumpan, obstaculicen o destruyan líneas o instalaciones de telecomunicaciones o la correspondencia postal, serán castigados con la pena de prisión de uno a cinco años*».

anche le reti digitali[630]. Tale reato è collocato tra i reati relativi al "disordine pubblico", per cui secondo alcuni è caratterizzato dalla presenza di un dolo specifico di alterazione del servizio pubblico[631]. Inoltre, si ritiene non sia sufficiente la mera produzione di un danno alle linee di telecomunicazione, ma è anche necessario che il danno sia relativo aduna parte rilevante del sistema di comunicazione e che sussista l'intenzione chiara e manifesta di causare un cortocircuito operativo del sistema[632].

Per quanto riguarda la conformità delle disposizioni tedesche sopra esaminate in relazione alla citata direttiva 2013/40/UE, la stessa dottrina tedesca rileva che le stesse rispettano i requisiti della direttiva quanto alle condotte sanzionate, ma non per le pene previste, che sono troppo basse rispetto agli standard richiesti dal legislatore europeo[633]. Inoltre, è stata criticata la mancata introduzione di una circostanza aggravante per sanzionare i casi in cui l'interferenza illecita relativamente ai sistemi e ai dati è stata commessa con furto di identità digitale (*Identitätsdiebstahls*), come previsto dall'art. 9 co. 5 della menzionata direttiva. Infatti, nonostante il furto di identità digitale possa essere senz'altro preso in considerazione come circostanza aggravante in sede di commisurazione della pena ai sensi del § 46 Abs. 2 StGB, si dubita che la mancata previsione espressa di un'ipotesi qualificata per sanzionare espressamente il furto d'identità digitale sia conforme alla direttiva[634]. Lo stesso, invece, non può dirsi affatto per la normativa spagnola, la quale ricalca pedissequamente il testo della menzionata direttiva e prevede anche una circostanza aggravante che sanziona il danneggiamento di dati o sistemi commesso con furto o indebito utilizzo dell'identità digitale altrui.

7. La responsabilità penale dei gestori di piattaforme illegali di scambio: il nuovo § 127 StGB

Il 1° ottobre 2021 è entrata in vigore nell'ordinamento tedesco la *Gesetz zur Änderung des Strafgesetzbuches – Strafbarkeit des Betreibens krimineller Handelsplattformen im Internet* del 12 agosto 2021, la quale ha completamente riscritto il previgente § 127 StGB, oggi intitolato "gestione delle piattaforme illegali di scambio su Internet" (*Betreiben krimineller Handelsplattformen im Internet*).

[630] FLORES PRADA I., *Criminalidad informática*, cit., p. 188.
[631] *Ibid*.
[632] *Ibid*.
[633] SIEBER U., *sub § 24 Computerkriminalität*, cit., p. 467.
[634] *Ibid*.

La nuova norma incriminatrice, che non ha omologhi né nell'ordinamento italiano, né in quello spagnolo, punisce, con la reclusione fino a cinque anni o la multa (*Geldstrafe*), salvo che il fatto costituisca un reato più grave, il gestore di una piattaforma illegale di scambio su *Internet*, costruita allo scopo di consentire o promuovere la commissione di atti illeciti[635]. La previsione legale ha l'obiettivo di punire lo scambio di oggetti e servizi illegali e/o di provenienza illecita su *Internet*, nonché di colmare le lacune normative che erano sorte in relazione al concorso di persone in alcuni reati cibernetici[636]. Tale norma, dunque, è volta a sanzionare il fenomeno del *cybercrime-as-a-service*, in particolare sia la fornitura di *software*, sia la fornitura o messa a disposizione dell'infrastruttura *hardware* per il funzionamento di queste piattaforme illegali[637].

Nell'introdurre la citata norma incriminatrice, il legislatore tedesco si è posto il problema dell'eventuale contrasto col principio di irresponsabilità penale degli *Internet Service Provider*, sancito, a livello europeo, dalla direttiva 2000/31/CE sul commercio elettronico. Tuttavia, la violazione della normativa europea è stata sin da subito esclusa, dal momento che per la menzionata direttiva lo Stato membro è tenuto a garantire l'irresponsabilità penale dell'*host provider* soltanto se quest'ultimo non è effettivamente a conoscenza dell'attività illegale. Ed in questo senso il § 127 StGB non solo richiede che il gestore della piattaforma *online* sia consapevole delle attività illegali ivi svolte, ma anche lo svolgimento del ruolo attivo della gestione, motivo per cui il privilegio di cui alla citata

---

635 «*Wer eine Handelsplattform im Internet betreibt, deren Zweck darauf ausgerichtet ist, die Begehung von rechtswidrigen Taten zu ermöglichen oder zu fördern, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist*. […]» (Chiunque gestisca una piattaforma di scambio su Internet, il cui scopo è quello di consentire o promuovere la commissione di atti illeciti, è punito con la reclusione non superiore a cinque anni o con una pena pecuniaria, salvo che il fatto costituisca più grave reato).

636 *Deutscher Bundestag Drucksache n. 19/28175 del 31 marzo 2021*, *Gesetzentwurf der Bundesregierung. Entwurf eines Gesetzes zur Änderung des Strafgesetzbuches – Strafbarkeit des Betreibens krimineller Handelsplattformen im Internet und des Bereitstellens entsprechender Server-Infrastrukturen*, p. 1. Come già evidenziato per l'ordinamento spagnolo, nell'ordinamento giuridico tedesco non esiste, a differenza di quanto avviene in Italia, il principio di unitarietà della responsabilità penale dei concorrenti nel reato, e si distingue, anche sul piano sanzionatorio, tra coautoria (*Täterschaft*) e partecipazione (*Teilnahme*). Coautore è colui che, assieme ad altri autori, compie direttamente l'atto (*Unmittelbarer Täter*), ha il dominio dello stesso ovvero agisce attraverso un intermediario o c.d. autore mediato (*Mittelbarer Täter*) e coloro che compiono congiuntamente l'atto (*Mittäter*). Nell'ambito della partecipazione si distingue tra istigazione (*Anstiftung*) e favoreggiamento (*Beihilfe*), che consiste nel rendere possibile la commissione del reato da parte del reo. Per una approfondita analisi critica della disciplina del concorso di persone nel reato nell'ordinamento tedesco v., per tutti, nella ormai sterminata letteratura, il lavoro monografico di ROXIN C., *Täterschaft und Tatherrschaft*, X ed., Berlin, 2019, *passim, c*ui si rinvia anche per i necessari riferimenti bibliografici; nonché i contributi di LAMPE E., *Tätersysteme: Spuren und Strukturen*, in *ZStW*, 2007, Vol. 119, n. 3, p. 471 ss. e KREUZBERG B., *Täterschaft und Teilnahme als Handlungsunrechtstypen. Zugleich ein Beitrag zur allgemeinen Verhaltensnormlehre*, Berlin, 2019, *passim*. Nella manualistica v. ROXIN C., *Strafrecht AT*, vol. II, cit., p. 1 ss. e p. 123 ss.; GROPP W., SINN A., *Strafrecht AT*, cit., p. 422 ss. e 464 ss.

637 *Ibid*., p. 11.

direttiva non opera[638]. Il § 127 StGB, dunque, punisce il fatto di chi gestisce e mantiene la propria infrastruttura virtuale allo scopo di consentire o promuovere i reati elencati dalla stessa norma, senza che vi sia alcuna connessione con i dati o le informazioni dell'utente pubblicati e memorizzati successivamente[639]. A tal proposito, va evidenziato che l'elemento soggettivo del reato in esame è il dolo, che può essere anche eventuale[640], per cui è necessario che il soggetto agente sia a conoscenza del fatto che la piattaforma è oggettivamente costituita o utilizzata per consentire o promuovere i reati elencati dalla norma e accetti il rischio della loro commissione.

L'originario progetto di legge di riforma del § 127 StGB prevedeva la punibilità del gestore della piattaforma *online* anche nel caso in cui la stessa fosse gestita in modo completamente automatizzato. Tale proposta fu oggetto di critiche, poiché avrebbe finito per punire anche il gestore della piattaforma di *trading* che non fosse stato a conoscenza delle specifiche operazioni ivi effettuate, in violazione del principio sancito dalla menzionata direttiva[641]. Per questo motivo, nel corso dei lavori preparatori, si decise di modificare la disposizione nei termini ora vigenti.

Il nuovo § 127 StGB tutela i beni giuridici della sicurezza e dell'ordine pubblico[642]. Si tratta di un reato di condotta, riconducibile alla categoria dei reati di pericolo astratto[643], avente natura permanente (*Dauerdelikt*)[644], posto che si consuma nel momento in cui la piattaforma viene chiusa o il gestore ne perde il controllo[645].

Il § 127, Abs. 1.2, StGB definisce gli quali sono gli "atti illeciti" la cui commissione deve essere favorita o facilitata attraverso la gestione della piattaforma ai fini della configurabilità del reato. Oltre a tutti i crimini (*Verbrechen*), vengono anche richiamati alcuni delitti (*Vergehen*), tra cui la truffa classica (§263 StGB), la *Computerbetrug* (§263a StGB), lo spionaggio (§ 202a StGB), l'intercettazione (§ 202b StGB) e la ricettazione di dati

---

638 WÜST M., *Die Underground Economy des Darknets*, cit., p. 72 ss.
639 KULHANEK T., *sub StGB § 127*, in B. von Heintschel-Heinegg (a cura di), *Beck-Online Kommentar Strafgesetzbuch*, VIII Edizione, München, 2022, Rn. 53 ss.
640 KULHANEK T., *sub StGB § 127*, cit., Rn. 50;
641 GERHOLD S.F., *Strafbarkeit des Betreibens krimineller Internethandelsplattformen*, in *ZRP*, 2021, p. 44 ss., p. 45.
642 EISELE J., *Schriftliche Stellungnahme zur Sachverständigenanhörung im Ausschuss für Recht und Verbraucherschutz des Deutschen Bundestages (BT-Drs. 19/28175)*, 2021, p. 1 ss., p. 2, disponibile *online* all'indirizzo
https://www.bundestag.de/resource/blob/838700/b7ac31fd95c417ab9f52266f5f06f50c/stellungnahme-eisele-data.pdf.
643 EISELE J., *Schriftliche Stellungnahme*, cit., p. 2; ZÖLLER M., *Die Strafbarkeit des Betreibens krimineller Handelsplattformen im Internet – Der neue § 127 StGB*, in *Int. Cybersecur. Law Rev.*, 2021, n. 2, p. 279 ss., p. 288.
644 EISELE J., *Schriftliche Stellungnahme*, cit., p. 9.
645 KULHANEK T., *sub StGB § 127*, cit., Rn. 71.

(§ 202d StGB), nonché gli atti preparatori allo spionaggio e all'intercettazione di dati (§ 202c StGB), l'alterazione di dati (§ 303a StGB), il sabotaggio informatico (§ 303b StGB), la falsificazione di dati rilevanti ai fini probatori (§ 269 StGB) e la contraffazione di carte di pagamento, assegni, cambiali e altri strumenti fisici di pagamento diversi dai contanti di cui al §152a StGB [646]. Tra essi, però, non è stato ricompreso il delitto di nuova introduzione di cui al § 152c StGB, che, come si è visto, punisce proprio colui che produce o si procura e programmi o dispositivi informatici al fine di commettere furto o indebito utilizzo di carte di credito.

Il § 127, Abs. 2, StGb fornisce una definizione legislativa di "piattaforma di scambio" (*Handelsplattform*) valida ai sensi della norma in esame, ovvero «*qualsiasi infrastruttura virtuale su Internet ad accesso libero oppure ad accesso limitato da protezioni tecniche, che consente la possibilità di offerta e scambio tra persone, beni, servizi commerciali o contenuti*»[647]. Di conseguenza, l'ambito di applicazione di tale norma non è limitato unicamente al *dark web*, ma può estendersi anche a piattaforme operanti nel *web* classico[648]. Il legislatore tedesco ha specificato che lo "scambio" (*Handel*) non dev'essere limitato allo scambio commerciale di beni, ma va inteso anche nel senso di baratto o, comunque, scambio reciproco, come avviene nella maggior parte delle piattaforme dedicate alla condivisione di materiale pedopornografico[649]. Alcuni problemi interpretativi sono sorti rispetto alle c.d. piattaforme a duplice uso o *dual use* (v. *supra*, cap. II, par. 1). L'ambito di applicazione della norma incriminatrice, secondo il suo tenore letterale, andrebbe, infatti, limitato soltanto alle piattaforme aventi come scopo oggettivo quello ivi indicato ("*deren Zweck daraus ausgereichtet ist*"). Una interpretazione troppo restrittiva della norma, però, rischierebbe, come sottolineato da un settore dottrinale, di creare una disparità di trattamento, dato che non potrebbe essere ricondotta nell'alveo del § 127 StGB la condotta del gestore di tali piattaforme che favorisca consapevolmente la commissione dei reati indicati perché progetta consapevolmente alcune parti della piattaforma per consentire e/o promuovere i corrispondenti reati indicati nel § 127 StGB, qualora la stessa abbia parallelamente funzioni lecite[650]. Sarebbe così possibile per i criminali informatici aggirare facilmente la norma ed

[646] Il § 152b StGB, avendo una pena minima di un anno di reclusione, è un crimine; perciò, è implicitamente ricompreso nel catalogo di reati.
[647] «*Handelsplattform im Internet im Sinne dieser Vorschrift ist jede virtuelle Infrastruktur im frei zugänglichen wie im durch technische Vorkehrungen zugangsbeschränkten Bereich des Internets, die Gelegenheit bietet, Menschen, Waren, Dienstleistungen oder Inhalte (§ 11 Absatz 3) anzubieten oder auszutauschen*».
[648] KULHANEK T., *sub StGB § 127*, cit., Rn. 1.
[649] *Deutscher Bundestag Drucksache n. 19/28175*, cit., p. 16.
[650] BRODOWSKI D., *Stellungnahme zum Gesetzentwurf der Bundesregierung: Entwurf eines Gesetzes zur Änderung des Strafgesetzbuches – Strafbarkeit des Betreibens krimineller Handelsplattformen im Internet und*

evitare la responsabilità penale[651]. Non pare persuasiva neppure la proposta di classificare la piattaforma o il sito come "criminale" per il solo fatto che al suo interno possano venirsi a trovare, anche per un breve lasso di tempo, alcune isolate offerte dal contenuto illecito[652]. Per ovviare a tali criticità, in dottrina si è proposto di non effettuare una valutazione aproristica delle piattaforme *online*, ritenendo più corretto procedere ad una valutazione caso per caso. A sostegno di tale tesi, si è richiamato il fatto che la formulazione della norma incriminatrice richiede che la piattaforma abbia come scopo principale quello di consentire o promuovere la commissione di atti illeciti, essendo sufficiente che sia, anche solo parzialmente, uno dei suoi scopi[653].

Il § 127, Abs. 3, StGB contempla una circostanza aggravante per colui che «*agisce professionalmente o come membro di un'associazione a delinquere che si è costituita allo scopo di commettere tali illeciti in modo continuativo*»[654]. Lo scopo di tale previsione consiste nel punire più gravemente i casi in cui la piattaforma venga impiegata per uno scopo di lucro, nonché la maggior pericolosità sociale derivante dal suo impiego nell'ambito di un'associazione a delinquere[655]. Tra le attività professionali/commerciali richiamate dalla disposizione rientrano anche le piattaforme di *hacking-as-a-service*, spazi virtuali in cui gli *hacker-tools* vengono venduti dietro corrispettivo, vale a dire a scopo di lucro[656].

Si è evidenziato come il rapporto tra questa ipotesi aggravata ed il reato base sia controverso, perché, di regola, i gestori di piattaforme di questo tipo, nonché coloro che forniscono le infrastrutture *server* a tal scopo, agiscono professionalmente su modello di *business* commerciale, ovvero nell'ambito di associazioni a delinquere (*Bande*), vale a dire da sodalizi che, secondo la normativa tedesca, devono essere composti da almeno tre persone che si sono unite con l'intenzione di commettere in futuro, e per un certo periodo di tempo, reati di diversa natura tra quelli indicati dalla legge[657]. Di conseguenza, questa ipotesi di

des Bereitstellens entsprechender Server-Infrastrukturen (BT-Drs. 19/28175), 2021, p. 1 ss., p. 4, disponibile *online* all'indirizzo https://kripoz.de/wp-content/uploads/2021/05/stellungnahme-brodowski-betreiben-kriminaller-handelsplattformen.pdf.

[651] EISELE J., *Schriftliche Stellungnahme*, cit., p. 7.

[652] KUSCHE C., *Die Strafbarkeit des Betreibens krimineller Handelsplattformen im Internet nach künftigem Recht*, in *JZ*, 2021, n. 1, p. 27 ss., p. 33.

[653] KULHANEK T., *sub StGB § 127*, cit., Rn. 40.

[654] «*Mit Freiheitsstrafe von sechs Monaten bis zu zehn Jahren wird bestraft, wer im Fall des Absatzes 1 gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung solcher Taten verbunden hat*».

[655] *Deutscher Bundestag Drucksache n. 19/28175*, cit., p. 17.

[656] EISELE J., *Schriftliche Stellungnahme*, cit., p. 8.

[657] BGH, sentenza 2 giugno 2021 – 3 StR 21/21.

reato qualificata viene a sovrapporsi a quella base, il cui ambito di applicazione finisce per diventare residuale[658].

Il § 127, Abs.4, StGB punisce con la pena della reclusione da un anno a dieci anni il fatto di chi «*nel commettere un atto illecito ai sensi del comma 1, agisce con il fine o comunque con la consapevolezza che la piattaforma commerciale su Internet abbia lo scopo di consentire o promuovere il delitto*»[659]. Anche in questo caso valgono le considerazioni svolte in relazione al controverso rapporto con la fattispecie base, dato che si può presumere che il gestore di una piattaforma sia di solito ben informato su ciò che accade nel suo mercato virtuale[660].

Al fine di regolare il rapporto con gli altri reati, è stata inserita una clausola di sussidiarietà espressa, che prevede la non applicabilità della norma in esame nel caso in cui il fatto costituisca un diverso reato punito più gravemente e che trova applicazione anche agli Abs. 3 e 4 § 127 StGB[661]. Ne consegue la configurabilità di un concorso tra il §127 StGB ed i reati da esso richiamati, data la parziale identità tra la condotta sanzionata dalla norma e gli atti esecutivi dei reati ivi elencati. In tal caso verrebbe a configurarsi unità di azione ai sensi del § 52 StGB, sempre che il reato sia punito meno gravemente rispetto al § 127 StGB[662]. Nel caso in cui quest'ultimo reato venga a concorrere coi successivi reati commessi e agevolati dalla piattaforma, si dovrebbe apprezzare un concorso materiale ai sensi del § 53 StGB[663]. Si è sostenuto, tra i primi commentatori, che la presenza della menzionata clausola di sussidiarietà si giustificherebbe per il fatto che il reato in esame ha natura di reato permanente, per cui la responsabilità penale di cui al § 127 StGB non potrebbe integrarsi unitamente a quella per i reati successivamente commessi, dato che se così fosse verrebbe meno la sua ragion d'essere[664]. Un diverso filone dottrinale sostiene, di contro, che la previsione della menzionata clausola venga di fatto a confermare che in realtà nell'ordinamento tedesco, prima della riforma del § 127 STGB, non sussisteva alcun vuoto normativo e che in questo modo il legislatore ha voluto evitare di creare un ingiustificato privilegio per coloro che, in mancanza di tale nuova norma incriminatrice, sarebbero stati chiamati a rispondere a titolo di concorso in uno dei reati di cui all'elenco, con l'applicazione

[658] ZÖLLER M., *Die Strafbarkeit des Betreibens krimineller*, cit., p. 293.
[659] «*Mit Freiheitsstrafe von einem Jahr bis zu zehn Jahren wird bestraft, wer bei der Begehung einer Tat nach Absatz 1 beabsichtigt oder weiß, dass die Handelsplattform im Internet den Zweck hat, Verbrechen zu ermöglichen oder zu fördern*».
[660] ZÖLLER M., *Die Strafbarkeit des Betreibens krimineller*, cit., p. 293.
[661] KULHANEK T., *sub StGB § 127*, cit., Rn. 76.
[662] *Ibid*., Rn. 79.
[663] *Ibid*., Rn. 80.
[664] EISELE J., *Schriftliche Stellungnahme*, cit., p. 9.

di una sanzione più elevata[665]. In virtù della disposizione di cui al § 5 n. 5a lett. b) StGB l'autore del reato deve essere di nazionalità tedesca o comunque essere domiciliato in Germania. Di conseguenza, i casi di gestione di una piattaforma fuori dalla Germania da parte di cittadini non tedeschi e allo stesso tempo ivi non domiciliati non rientrano nell'ambito applicativo del §127 StGB[666]. Questa disposizione, dunque, finisce per rendere inapplicabile tale reato ad un rilevante numero di casi, dato che, come si è esaminato, le piattaforme di *cybercrime-as-a-service* spesso operano a livello globale.

7.1. Segue: sull'opportunità di introdurre una fattispecie incriminatrice di ugual tenore nell'ordinamento italiano

Qualche perplessità potrebbe sorgere in merito all'opportunità di introdurre una analoga norma incriminatrice anche nell'ordinamento italiano. Come evidenziato, per quanto concerne la disciplina penale del concorso di persone nel nostro Paese vige la clausola generale di cui all'art. 110 c.p., che, a differenza di quanto previsto in Germania, sancisce il principio della pari responsabilità dei concorrenti. In forza di tale clausola, le condotte previste dal § 127 StGB potrebbero pertanto già essere punite a titolo di concorso di persone nel reato. La previsione, in prospettiva *de jure condendo*, di una norma analoga nel nostro sistema penale rischierebbe pertanto di dar vita ad un'ipotesi di reato che, senza alcuna giustificazione politico-criminale, verrebbe a costituire una deroga alla disciplina generale sul concorso di persone nel reato. Verrebbe poi a configurarsi il rischio di un ingiustificato privilegio per i gestori delle piattaforme, mediante la previsione di un autonomo reato a soggettività ristretta, sanzionato con pena più lieve rispetto a quella che si dovrebbe applicare qualora il reo fosse chiamato a rispondere a titolo di concorso nei reati espressamente elencati dalla norma. Difficile, inoltre, ipotizzare *de jure condendo* la previsione nel nostro ordinamento di una norma penale ad hoc con un ambito applicativo più ampio o comunque diverso rispetto alla fattispecie tedesca, in quanto verrebbe a contrastare col generale principio di derivazione europea di irresponsabilità penale degli *Internet Service Provider*, di cui si è detto in precedenza. In conclusione, sarebbe opportuno riflettere sulla opportunità di adottare un cambio di strategia a livello europeo, in linea con quanto stabilito nella proposta europea per l'adozione del c.d. *Digital Service Act*[667], che prevede l'aggiornamento

[665] ZÖLLER M., *Die Strafbarkeit des Betreibens krimineller*, cit., p. 290.
[666] *Deutscher Bundestag Drucksache n. 19/28175*, cit., p. 3 e 26.
[667] Proposta di regolamento del Parlamento europeo e del Consiglio relativo a un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE, COM (2020) 825 final, 15 dicembre 2020.

della disciplina in materia di responsabilità dei prestatori di servizi della società dell'informazione nonché l'adozione di obblighi in capo ai prestatori di servizi per il contrasto ai contenuti illeciti in rete.

In linea con quanto sostenuto da un autorevole settore della dottrina tedesca, la diffusione di piattaforme *online* dedite alla vendita di beni e servizi illegali o di illecita provenienza è un fenomeno diffuso a livello transnazionale. Di conseguenza, tale settore dovrebbe essere regolato dal legislatore europeo, ai sensi dell'art. 83, par. 1.2, TFUE, il quale dovrebbe intervenire per fissare dei principi in materia, in particolare per quanto riguarda la possibilità per le autorità di *law enforcement* di non oscurare immediatamente una piattaforma di questo tipo, in modo da poter continuare a "vigilarla" per fini investigativi, in modo da poter individuare venditori e acquirenti[668].

8. La disciplina penale del riciclaggio

Come già evidenziato, non sono solo gli attacchi informatici contro il patrimonio ad essere diffusi globalmente, ma anche il successivo reimpiego dei capitali illecitamente ottenuti tramite gli stessi. È opportuna, dunque, anche un'analisi della disciplina penale in materia di riciclaggio dei due ordinamenti sopra esaminati, anche con riferimento alla responsabilità dei *financial manager*.

Nel diritto penale tedesco il riciclaggio è punito dal § 261 StGB. Tale norma fu introdotta nel codice penale tedesco con la Legge per la lotta al traffico illegale di droga e ad altre forme di criminalità organizzata del 15 luglio 1992 (*Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität* - OrgKG). In questo modo, il legislatore tedesco ha adempiuto agli obblighi internazionali che prevedevano l'obbligo di sanzionare penalmente il riciclaggio di denaro, in particolare la prima direttiva sul riciclaggio di denaro 91/308/CEE del 10 giugno 1991.

Nell'ordinamento spagnolo, invece, il reato di *blanqueo* è sanzionato dall'art. 301 del *código penal* sin dal 1995. È stato oggetto di modifiche sia da parte della *Ley Orgánica* 15/2003 del 25 novembre che della successiva *Ley Orgánica* 5/2010 del 22 giugno. Quest'ultima norma, in particolare, ha modificato la rubrica del capitolo XIV del titolo XIII del libro II, che oggi è intitolato "*De la receptación y el blanqueo de capitales*". Infine, la *Ley Orgánica* 6/2021 del 28 aprile, di attuazione della direttiva 2018/1673/UE del 23 ottobre 2018 sulla lotta al riciclaggio mediante il diritto penale ha aggiunto una nuova circostanza

[668] BRODOWSKI D., *Stellungnahme zum Gesetzentwurf*, cit., p. 2.

aggravante speciale, per il caso in cui i beni provengano da uno dei reati ivi indicati, tra cui, però, non sono ricompresi quelli contro il patrimonio, mentre all'art. 302 c.p. ha previsto una circostanza aggravante soggettiva per i soggetti che, obbligati ai sensi della normativa antiriciclaggio e anticorruzione, commettano una qualsiasi delle condotte di riciclaggio descritte nell'art. 301 c.p. agendo nell'ambito della loro attività professionale[669].

Anche se il §261 StGB è collocato tra i *Vermögensdelikte*, vi è a tutt'oggi dibattito in merito a quale sia il bene giuridico tutelato da quest'ultima norma[670]. Addirittura, la stessa Corte costituzionale tedesca non è riuscita a identificare quale sia e ha definito come "vaghi" i tentativi sino a quel momento compiuti per determinarlo[671].

Alcuni autori sostengono che il reato in questione tuteli l'amministrazione della giustizia[672], altri l'integrità del mercato monetario e finanziario[673], altri ancora il bene giuridico tutelato dal reato presupposto[674], oppure il ciclo economico e finanziario e l'economia nazionale[675] oppure la sicurezza interna nazionale[676]. Infine, vi è chi ritiene si tratti di reato plurioffensivito, per cui i beni giuridici protetti sarebbero la garanzia della confisca dei beni, la promozione delle attività investigative e la tutela dei beni giuridici tutelati dai reati presupposto[677].

---

669 ABEL SOUTO M., *El nuevo tipo agravado de blanqueo en el ejercicio profesional de los obligados por la normativa de prevención*, in *Revista penal México*, 2022, n. 20, p. 17 ss., p. 20 ss.

670 VOß M., *Die Tatobjekte der Geldwäsche*, Berlin, 2007, p. 8 ss.

671 BVerfG, sentenza 30 marzo 2004 – 2 BvR 1520/01: «*In Rechtsprechung und Literatur ist zwar umstritten, welchem Rechtsgut § 261 II Nr. 1 StGB dient. Ungeachtet der Frage aber, ob die Schutzrichtung der Strafvorschrift auf die inländische Rechtspflege, das Ermittlungsinteresse der Strafverfolgungsbehörden, den „legalen Wirtschafts- und Finanzkreislauf, die durch die Vortaten geschützten Rechtsgüter, die „innere Sicherheit" ausgerichtet ist oder ob sie den Schutz eines nicht näher konkretisierten Rechtsguts eigener Art bezweckt, muss eine Widerlegung des durch die herkömmlichen Methoden gefundenen Auslegungsergebnisses schon an der Weite und Vagheit der durch die Strafvorschrift möglicherweise geschützten Rechtsgüter scheitern*» (In giurisprudenza e in dottrina è ancora controverso quale sia l'interesse giuridico tutelato dal § 261 II n. 1 StGB. A prescindere dalla questione se la norma penale sia rivolta alla tutela dell'amministrazione della giustizia, dell'interesse investigativo delle autorità inquirenti, al "ciclo economico-finanziario legale", dei beni giuridici tutelati dai reati presupposto, della "sicurezza interna" o di un interesse giuridico proprio non meglio specificato, dev'essere confutato qualsiasi un risultato interpretativo cui si è pervenuti con i metodi convenzionali, a causa dell'ampiezza e della vaghezza degli interessi giuridici eventualmente tutelati dalla norma penale).

672 NESTLER N., *Bank- und Kapitalmarktstrafrecht*, Heidelberg, 2016, p. 356.

673 NEUHEUSER S., *StGB § 261 Geldwäsche; Verschleierung unrechtmäßig erlangter Vermögenswerte*, in *Münchener Kommentar zum StGB*, 2021, IV ed., Rn. 12.

674 LEIP C., *Der Straftatbestand der Geldwäsche - Zur Auslegung des § 261 StGB*, 1999, Berlin, p. 46 ss.

675 LAMPE E., *Der neue Tatbestand der Geldwäsche (§ 261 StGB)*, in *JZ*, 1994, p. 123 ss., p. 125 s.

676 BARTON S., *Sozial übliche Geschäftstätigkeit und Geldwäsche (§ 261 StGB)*, in *StV*, 1993, n. 3, p. 156 ss., p. 160.

677 RASCHKE A., *Geldwäsche und rechtswidrige Vortat – Eine Analyse der Irrtumsproblematik am Beispiel der Geldwäsche*, 2014, Baden-Baden, p. 49 s.

Nell'ordinamento spagnolo, nonostante il dibattito in merito[678], la dottrina maggioritaria ritiene si tratti di un reato plurioffensivo, i cui beni giuridici tutelati sono l'ordine socio-economico[679] e l'amministrazione della giustizia[680].

Il § 261 StGB è stato recentemente modificato dall'articolo 1 della legge per il miglioramento della lotta riciclaggio di denaro attraverso il diritto penale del 9 marzo 2021 (*Gesetz zur Verbesserung der strafrechtlichen Bekämpfung der Geldwäsche - GwStrRVG*). Questa complessa fattispecie è stata ampiamente rielaborata e ora contiene dieci paragrafi. La modifica più significativa consiste nell'abbandono del precedente catalogo dei reati presupposto, per cui oggi qualsiasi reato può essere presupposto del riciclaggio. Il legislatore tedesco, dunque, come già fece a suo tempo quello italiano, ha optato per il c.d. paradigma *all-crimes*[681]. Tale cambiamento è stato accolto con sfavore da una parte della dottrina, perché comporta un significativo ampliamento della responsabilità penale. La prima critica mossa è che l'inclusione di reati bagatellari nel catalogo dei reati presupposto rischia di far perdere di vista l'obiettivo di un migliore e più efficace sanzione dei reati di riciclaggio[682]. Ulteriore critica sollevata è che l'estensione del campo di applicazione del riciclaggio di denaro a tutti i reati sarebbe in conflitto con il principio di proporzionalità, perché ora ogni reato minore potrebbe potenzialmente essere alla base di un altro reato di riciclaggio di denaro[683]. A tali critiche si può però obiettare che il paradigma *all-crimes* è già stato adottato da tempo in molti paesi, tra cui l'Italia, ove non sembra che i rischi ivi profetizzati si siano

---

[678] Per una sintesi delle diverse posizioni v. FARALDO CABANA P., *Aspectos básicos del delito de blanqueo de bienes en el Código penal del 1995*, in *Estudios penales y criminológicos*, 1998, vol. 31, p. 117 ss., p. 124 ss. E MOLINA FERNÁNDEZ F., *¿Qué se protege en el delito de blanqueo de capitales?: reflexiones sobre un bien jurídico problemático, y a la vez aproximación a la «participación» en el delito*, in M. Bajo Fernández, S. Bacigalupo Saggese (a cura di), *Política Criminal y blanqueo de capitales*, cit., p. 91 ss., p. 109 ss.

[679] ALONSO PÉREZ F., *Delitos Contra el Patrimonio*, cit., p. 470.

[680] BLANCO CORDERO I., *El Delito de Blanqueo de Capitales*, Cizur Menor, 2015, p. 313; BAJO FERNÁNDEZ M., BACIGALUPO SAGGESE S., *Derecho penal económico*, Madrid, 2010, p. 721; CALDERÓN CEREZO A., CHOCLÁN MONTALVO J.A., *Manual de Derecho Penal. Tomo II Parte Especial*, Barcelona, 2005, p. 314. Anche in questo caso, tuttavia, non mancano opinioni dissenzienti. Infatti, per ARÁNGUEZ SÁNCHEZ C., *El Delito de Blanqueo de Capitales*, Madrid, 2000, p. 98 bene giuridico tutelato è la libertà di concorrenza. In giurisprudenza per Tribunal Supremo, sez. I penale, sentenza 2 marzo 2016, n. 165 trattasi di reato plurioffensivo, ove beni giuridici tutelati sono l'ordine socioeconomico, la tutela del commercio legale e l'amministrazione della giustizia. Sul punto v. anche MARTÍN SAGRADO O., *La determinación del bien jurídico protegido por el delito de blanqueo de capitales y el autoblanqueo. Un debate que no cesa*, in *Boletín del Ministerio de Justicia*, 2018, n. 2206, p. 1 ss., p. 7 ss.

[681] GAZEAS N., *Das neue Geldwäsche-Strafrecht: Weitreichende Folgen für die Praxis*, in *NJW*, 2021, p. 1041 ss., p. 1042.

[682] MÜLLER M., *Neufassung des Geldwäschetatbestands – Der "all-crimes-approach"*, in *NJW-Spezial*, 2021, p. 312 ss., p. 312.

[683] EL-GHAZI M., LAUSTETTER C., *Das Gesetz zur Verbesserung der strafrechtlichen Bekämpfung der Geldwäsche – Ein Überblick über die wichtigsten Änderungen beim Straftatbestand des § 261 StGB und bei der selbständigen Einziehung nach § 76 a Abs. 4 StGB*, in *NZWiSt*, 2021, p. 209 ss., p. 212; GAZEAS N., *Das neue Geldwäsche-Strafrech*., cit., p. 1044.

realizzati. Anzi, tale approccio consente una notevole semplificazione. Più che la presenza di un catalogo di reati presupposto, il vero *discrimen* è costituito dalla selezione delle condotte sanzionate.

Anche il legislatore spagnolo ha aderito al paradigma *all-crimes*, per cui reato presupposto può essere qualsiasi reato[684], anche colposo[685]. La norma, infatti, specifica che beni oggetto del riciclaggio devono costituire provento di una "precedente attività delittuosa"[686]. Mentre in precedenza si richiedeva che il reato presupposto fosse "grave", questo requisito è stato eliminato dalla *Ley Orgánica* n. 5/2010 cit. A tal proposito, la giurisprudenza del *Tribunal Supremo* ha precisato che non occorre l'esistenza di una previa condanna per il reato presupposto[687]. Per alcuni autori, addirittura, non è neppure necessario si tratti di un reato consumato, potendo essere qualsivoglia attività delittuosa che sta commettendo, o nella quale sta partecipando, lo stesso autore del riciclaggio[688]. L'adozione del paradigma *all-crimes*, dunque, accomuna tutti i tre paesi.

Molto diverso, invece, è il discorso con riferimento alle condotte sanzionate.

8.1. Le condotte sanzionate

Come sopra accennato, i reati di cui § 261 StGB sono stati recentemente riformati nel 2021. Le condotte precedentemente sanzionate dal precedente § 261 Abs. 2 StGB (*sich oder einem Dritten verschaffen* e *verwahren oder für sich oder einen Dritten verwenden*) sono oggi state trasferite nel § 261 StGB Abs. 1, ai n. 3 e 4. Il paragrafo 1 incrimina gli atti che impediscono o ostacolano le forze dell'ordine nel sequestro degli oggetti. Le ipotesi di cui al n. 1 Abs. 1 costituiscono un reato di pericolo astratto[689]. Il nuovo n. 2 dell'Abs. 1,

---

[684] BLANCO CORDERO I., *El Delito de Blanqueo de Capitales*, cit., p. 347 s. In tal senso già DÍEZ RIPOLLÉS J.L., *El blanqueo de capitales procedentes del trafico de drogas. La recepción de la legislación internacional en el ordenamiento penal español*, in *Actualidad penal*, 1994, n. 32, p. 582 ss., p. 609, sosteneva la necessità di abbandonare il catalogo dei reati presupposto: «*Debe de abandonarse la técnica de utilizar determinadas conductas delictivas previas como delitos de referencia, por más que en los últimos tiempos se registre una incorporación de nuevas infracciones. Será suficiente con el origen delictivo de los bienes económicos que se intentan introducir en el tráfico legal*». Si evidenzia che nel codice penale spagnolo, a differenza che in quello italiano e tedesco, non vi è distinzione tra le tipologie di reati, i quali sono tutti *delitos*. L'art. 13 *Código penal* distingue unicamente tra *delitos graves*, *delitos menos graves* e *delitos leves*.

[685] BLANCO CORDERO I., *El Delito de Blanqueo de Capitales*, cit., p. 384.

[686] ABEL SOUTO M., *Expansión española del blanqueo de dinero en la última década de reformas penales*, in S. Cornejo Aguiar (dir.), I.P. Guevara Vásquez (dir.), G. E. Piva Torres (coord.), *Selecciones de dogmática penal latinoamericana. Presente y futuro*, Barcelona, 2020, p. 381 ss., p. 388 contesta l'utilizzo del termine *actividad delictiva* in luogo di quello di *delito*, evidenziando che tale modifica, operata dalla riforma del 2010, non modifica in alcun modo il disvalore penale della norma, ma dà solo origine a contrasti interpretativi.

[687] Tribunal Supremo, sez. I penale, sentenza 29 settembre, n. 1704; Tribunal Supremo, sez. I penale, sentenza 14 febbraio 2003, n. 575; Tribunal Supremo, sez. I penale, sentenza 27 gennaio 2006, n. 141; Tribunal Supremo, sez. I penale, sentenza 13 dicembre 2005, n. 1426.

[688] MIRÓ LLINARES F., *La respuesta penal al ciberfraude*, cit., p. 37.

[689] NEUHEUSER S., *StGB § 261 Geldwäsche*, cit., Rn. 17.

invece, sanziona chi scambia, trasferisce o cede un oggetto che risulta essere provento di reato con l'intenzione di ostacolarne il ritrovamento, la confisca o l'identificazione della provenienza. Con l'introduzione di questa disposizione vi è stata un'anticipazione della punibilità, perché oggi lo scambio dell'oggetto incriminato, il suo trasferimento o la sua cessione sono ora già punibili se l'autore del reato agisce con il dolo specifico richiesto. Trattasi, dunque, anche in questo caso di reato di pericolo astratto, poiché in questo caso non è richiesto né il verificarsi della sparizione del bene né un pericolo concreto in tal senso[690].

I nuovi n. 3 e 4 Abs. 1 sanzionano le condotte di procacciamento, custodia e uso. Si tratta anche in questo caso di reato di mera condotta e di pericolo astratto[691]. Il procacciamento è l'assunzione consapevole e deliberata del potere di disporre del bene da parte dell'autore del reato per i propri scopi attraverso l'acquisizione derivata e la cooperazione consensuale con l'autore del reato presupposto[692]. Per custodia, invece, si intende la presa in consegna o la detenzione di un oggetto al fine di conservarlo per un terzo o per un proprio uso successivo e in tale nozione rientra l'uso di qualsiasi oggetto idoneo al riciclaggio di denaro in conformità alla sua destinazione[693]. Il nuovo par. 2 non richiede più che l'origine dell'oggetto sia effettivamente occultata, ma è sufficiente occultare fatti che possono avere rilevanza per evitare che l'oggetto sia rintracciato, confiscato o comunque ne venga determinata l'origine. Questa modalità del reato non è del tutto nuova e si ricollega alla precedente modalità di occultamento di cui alla precedente versione della norma[694]. Pertanto, anche in questo caso può essere classificato come reato di pericolo astratto[695].

Dunque, ormai tutte le condotte sopra descritte costituiscono reati di pericolo astratto, con conseguente anticipazione della responsabilità penale[696]. Ancora non è stato chiarito che

---

690 BT-Dr. 19/24180, p. 30 s. «*Eine konkrete Gefährdung dieser Erfolge ist jedoch nicht erforderlich, so dass es sich bei Nummer 2 um ein abstraktes Gefährdungsdelikt handelt*» (Tuttavia, questi eventi non richiedono una concreta messa in pericolo, per cui il numero 2 è un reato di pericolo astratto).

691 NESTLER N., *Bank – und Kapitalmarktstrafrecht*, cit., p. 358.

692 *Ibid*.

693 RUHMANNSEDER F., *StGB § 261 Geldwäsche*, in B. Von Heintschel-Heinegg, *BeckOK StGB*, cit., Rn. 27 e 28.

694 EL-GHAZI M., LAUSTETTER C., *Das Gesetz zur Verbesserung der strafrechtlichen Bekämpfung der Geldwäsche – Ein Überblick über die wichtigsten Änderungen beim Straftatbestand des § 261 StGB und bei der selbständigen Einziehung nach § 76 a Abs. 4 StGB*, in *NZWiSt*, 2021, p. 209 ss., p. 209.

695 Nella motivazione della legge si specifica che «*Dagegen sind den Handlungen des Absatzes 2 bereits die Gefährdungen immanent, denn es sind gerade keine neutralen, sondern auf Manipulation ausgerichtete Handlungen*» (Al contrario, nelle condotte di cui all'Abs. 2 è intrinseco il pericolo, perché appunto non sono atti neutrali, ma finalizzati alla manipolazione), v. BT-Dr. 19/24180, p. 33. Nello stesso senso anche ALTENHAIN K., FLECKENSTEIN L., *Der Gesetzentwurf zur Neufassung des § 261 StGB*, in *JZ*, 2020, n. 21, p. 1045 ss., p. 1049.

696 BÜLTE J., *Stellungnahme zum Entwurf eines Gesetzes zur Verbesserung der strafrechtlichen Bekämpfung der Geldwäsche, Ausschuss für Recht und Verbraucherschutz des Deutschen Bundestages am 9. Dezember 2020*, disponibile *online* al sito

cosa si intenda per "occultamento"[697]. A tal proposito, si evidenzia che la relazione introduttiva alla legge evidenzia che sia l'occultamento che la dissimulazione richiedono «*macchinazioni concretamente fuorvianti e attivamente soppressive relative a tutti i fatti che possono essere rilevanti per le autorità inquirenti nelle indagini e nella confisca*»[698]. Motivo per cui i primi commentatori hanno ritenuto che l'occultamento non possa consistere nell'omissione di qualsiasi fatto che avrebbe facilitato la localizzazione, la confisca o la determinazione dell'origine di un bene[699].

Anche la disposizione di cui all'art. 301 *Código penal* è suddivisa in diversi commi. Nel primo si sanzionano le condotte da compiere per occultare o coprire l'origine illecita dei beni o per fornire aiuto all'autore del reato presupposto[700]. Condotte sanzionate, dunque, sono l'acquisto, il possesso, l'utilizzo, la conversione e la trasmissione, nonché la realizzazione di qualsiasi altro atto per occultare o coprire l'illegittima provenienza dei beni in questione o aiuta la persona che ha partecipato alla commissione del reato presupposto ad andare esente da responsabilità penale.

Trattasi di norma a più fattispecie, per cui l'integrazione di più condotte descritte da parte del reo dà luogo ad un unico reato[701]. Data la formulazione poco chiara della norma, si sono contrapposte due tesi. Per la prima l'art. 301.1 c.p. sanziona la mera acquisizione, conversione o trasferimento di beni con la consapevolezza della loro origine criminale, e la commissione di qualsiasi altro atto allo scopo di nascondere o dissimulare la loro origine illegale o di aiutare la persona che ha commesso il reato presupposto a conseguire l'impunità per i suoi atti[702]. Per altri autori, invece, la trasmissione, così come qualsiasi altro atto, è punibile solo quando viene effettuata allo scopo di nascondere o mascherare l'origine illecita dei beni, o per aiutare la persona che ha commesso il reato a conseguire l'impunità[703],

---

https://www.bundestag.de/resource/blob/810652/881114134916dc4b59a8cdeacb511623/buelte_neu-data.pdf, p. 24 s.

[697] EL-GHAZI M., LAUSTETTER C., *Das Gesetz zur Verbesserung der strafrechtlichen Bekämpfung der Geldwäsche*, cit., p. 213.

[698] BT-Dr. 19/24180, cit., p. 33.

[699] EL-GHAZI M., LAUSTETTER C., *Das Gesetz zur Verbesserung der strafrechtlichen Bekämpfung der Geldwäsche*, cit., p. 213.

[700] «*El que adquiera, posea, utilice, convierta, o transmita bienes, sabiendo que éstos tienen su origen en una actividad delictiva, cometida por él o por cualquiera tercera persona, o realice cualquier otro acto para ocultar o encubrir su origen ilícito, o para ayudar a la persona que haya participado en la infracción o infracciones a eludir las consecuencias legales de sus actos, será castigado con la pena de prisión de seis meses a seis años y multa del tanto al triplo del valor de los bienes*».

[701] ABEL SOUTO M., *El delito de blanqueo en el Código penal español. Bien juridico protegido, conductas típicas y objecto material tras la Ley orgánica 15/2003, de 25 de noviembre*, Barcelona, 2005, p. 102.

[702] *Ibid*., p. 94.

[703] DEL CARPIO DELGADO J., *La posesión y utilización como nuevas conductas en el delito de blanqueo de capitales*, in *Revista General de Derecho Penal*, 2011, n. 15, p. 1 ss., p. 11; FARALDO CABANA P., *Aspectos*

interpretazione, quest'ultima, che restringe l'ambito applicativo della norma. L'acquisizione viene interpretata in senso ampio e intesa come l'esercizio di diritti sui proventi del reato[704], la conversione come sostituzione di un bene con un altro[705], mentre il trasferimento come lo spostamento della cosa da un luogo ad un altro, l'alienazione, la trasmissione o trasferimento di beni a terzi[706]. Oltre a ciò, vi è la clausola di chiusura, che prevede la punibilità della realizzazione di "qualsiasi altro atto" volto a realizzare qualsiasi altro atto per occultare o coprire l'illegittima provenienza dei beni in questione o ad aiutare la persona che ha partecipato alla commissione del reato presupposto ad andare esente da responsabilità penale, formula ampia che richiede unicamente la presenza di un determinato fine dell'agire[707].

Le condotte del possesso e dell'utilizzazione sono state inserite nella norma a seguito della riforma di cui alla *Ley Orgánica* 5/2010 cit. Tale aggiunta è stata oggetto di critiche sia perché non sono propriamente condotte di riciclaggio, visto che non presuppongono alcun cambio di titolarità o comunque occultamento dei beni indicati, dilatando così in modo eccessivo l'ambito applicativo della fattispecie[708]. La giurisprudenza, pertanto, nel tentativo di limitare l'ambito applicativo della fattispecie, richiedendo che il possesso o l'utilizzo siano commessi con l'intenzione di occultare o nascondere[709] e sostenendo che la formula "qualsiasi altro atto" richiede che le condotte si traducano in operazioni dirette sui beni di provenienza illecita, compiute personalmente o per interposta persona[710].

Per alcuni autori il co. 1 in questione in realtà sanzionerebbe in modo autonomo il tentativo di favoreggiamento reale[711]. Per altri ancora le condotte che costituiscono riciclaggio vero e proprio sarebbero solo quelle di cui al co. 2, per cui il co. 1 sanziona in modo autonomo il tentativo e gli atti preparatori alla commissione del riciclaggio[712]. Per

básicos del delito de blanqueo de bienes en el Código penal del 1995, cit., p. 139; PALMA HERRERA J.M., *Los delitos de blanqueo de capitales*, Madrid, 2000, p. 418.

[704] BLANCO CORDERO I., *El Delito de Blanqueo de Capitales*, cit., p. 549; PALMA HERRERA J.M., *Los delitos de blanqueo de capitales*, cit., p. 421.

[705] PALMA HERRERA J.M., *Los delitos de blanqueo de capitales*, cit., p. 429.

[706] *Ibid*., p. 459.

[707] FARALDO CABANA P., *Aspectos básicos del delito de blanqueo de bienes en el Código penal del 1995*, cit., p. 142. ARÁNGUEZ SÁNCHEZ C., *El Delito de Blanqueo de Capitales*, cit., p. 227 evidenzia che tale clausola non è rispettosa del principio di tassatività in materia penale, perché eccessivamente ampia.

[708] MUÑOZ CONDE F., *Derecho Penal*, cit., p. 556.

[709] Così Tribunal Supremo, sez. II penale, sentenza 29 aprile 2015, n. 265. In tal senso anche DEL CARPIO DELGADO J., *La posesión y utilización como nuevas conductas en el delito de blanqueo de capitales*, cit., p. 21.

[710] Tribunal Supremo, sez. I penale, sentenza 26 novembre 2014, n. 809.

[711] BLANCO CORDERO I., *El Delito de Blanqueo de Capitales*, cit., p. 312.

[712] LASCURAÍN SÁNCHEZ J.A., *Blanqueo de capitales*, in *Derecho penal económico y de la empresa*, cit., p. 493 ss., p. 504.

determinare se si tratta di reato di mera condotta o di evento bisogna differenziare tra le diverse condotte previste: nel caso dell'acquisizione è di evento perché richiede l'incorporazione del bene o del diritto sopra il patrimonio, così nel caso della conversione, che richiede la trasformazione del bene, mentre la trasmissione costituisce un reato di evento che richiede un trasferimento patrimoniale. La realizzazione di qualsiasi atto sul bene, invece, non chiedendo l'occultamento o la dissimulazione, costituisce reato di mera condotta[713].

Il co. 2, invece, sanziona colui che occulta o dissimula i beni[714]. In questo caso, trattasi di reato di evento[715]. L'occultamento consiste nel nascondere, camuffare, coprire o tacere su ciò che si conosce, in modo da evitare che terzi vengano a conoscenza della natura, dell'origine, dell'ubicazione, destinazione, movimenti o dei diritti esistenti sui beni di provenienza illecita[716]. Per dissimulazione (*encubrimiento*), va evidenziato che lo stesso trova definizione legislativa nell'art. 451 c.p., ovvero assistenza, favoreggiamento reale o aiuto con riferimento alla cosa e favoreggiamento personale o aiuto alla persona del colpevole[717]. Essa include, dunque, il nascondere, l'alterazione e la distruzione totale o parziale del bene al fine di nasconderne l'origine, l'ubicazione, la destinazione, i movimenti, ecc. La relazione tra i due commi è di alternatività[718].

Nonostante la loro eterogeneità, appare evidente che le condotte sanzionate sono molto più numerose di quelle descritte negli artt. 648-*bis* e 648-*ter* c.p. e che la soglia di rilevanza penale è notevolmente anticipata.

8.2. L'oggetto del reato

Per quanto riguarda l'oggetto del reato di riciclaggio, nella norma tedesca esso può essere qualsiasi oggetto (*Gegenstand*), non solo il denaro, ma anche qualsiasi altro bene[719]. Ci si pone, dunque, il problema se le criptovalute possano essere considerate "*Gegenstand*" e, dunque, essere oggetto del reato di riciclaggio. La dottrina tedesca evidenzia che il termine

[713] BLANCO CORDERO I., *El Delito de Blanqueo de Capitales*, cit., p. 546; ABEL SOUTO M., *El delito de blanqueo en el Código penal español*, cit., p. 111, 116 e 121.
[714] «*Con las mismas penas se sancionará, según los casos, la ocultación o encubrimiento de la verdadera naturaleza, origen, ubicación, destino, movimiento o derechos sobre los bienes o propiedad de los mismos, a sabiendas de que proceden de alguno de los delitos expresados en el apartado anterior o de un acto de participación en ellos*».
[715] BLANCO CORDERO I., *El Delito de Blanqueo de Capitales*, cit., p. 615; PALMA HERRERA J.M., *Los delitos de blanqueo de capitales*, cit., p. 463.
[716] BLANCO CORDERO I., *El Delito de Blanqueo de Capitales*, cit., p. 617.
[717] *Ibid*., p. 620.
[718] Tribunal Supremo, sez. I penale, sentenza 19 febbraio 2002, n. 155.
[719] NESTLER N., *Bank- und Kapitalmarktstrafrecht*, Heidelberg, 2017, p. 359.

"oggetto" per definizione comprende solo cose (*Sachen*) e diritti (*Rechte*)[720]. Se il *Token* rappresenta un diritto virtuale, basti pensare ad esempio ai *Security Token*, può essere considerato come oggetto. Quest'operazione ermeneutica, tuttavia, è più difficile da compiere coi *Token* che non rappresentano nessun "diritto", ovvero i *Currency Token* quali *Bitcoin*, *Monero* e *ZCash*, dato che gli stessi non costituiscono né cose materiali, né diritti. Tuttavia, la stessa dottrina evidenzia che non necessariamente il concetto di "*Gegenstands*" di cui al § 261 StGB dev'essere interpretato in modo così rigido, ma è possibile interpretarlo estensivamente ritenendo oggetto «*qualsiasi posizione patrimoniale delimitabile con funzione di esclusione*»[721]. A tal proposito, si evidenzia che il titolo ufficiale della disposizione utilizza il termine "valore patrimoniale" (*Vermögenswert*), che indica la possibilità di interpretare il concetto di oggetto senza ritenere che esso coincida con le cose materiali e i diritti[722]. L'intenzione del legislatore, infatti, è quella di far rientrare nel campo applicativo del § 261 StGB il più ampio numero di valori patrimoniali possibili[723]. Poiché le criptovalute si prestano bene a compiere il riciclaggio di beni di provenienza illecita, grazie alle loro proprietà tecniche, l'esclusione delle stesse dall'ambito di applicazione del § 261 StGB si tradurrebbe in una lacuna di responsabilità penale estremamente facile da sfruttare, in contrasto con lo scopo legislativo. Di conseguenza, non si può che ritenere che anche le criptovalute siano ricomprese nella definizione di *Gegenstand* di cui al § 261 Abs. 1 S. 1 StGB[724].

Nella corrispondente fattispecie spagnola, invece, l'oggetto del reato è costituito dai beni, ovvero qualunque beneficio economicamente valutabile[725]. Nella nozione di beni, dunque, sono ricompresi sia beni mobili che immobili, sia materiali che immateriali, diritti o valori e crediti[726]. Si ritiene possa essere oggetto del riciclaggio anche l'oggetto materiale del reato presupposto, quando questo sia economicamente valutabile, assimilabile al patrimonio e quando l'esecuzione degli atti di riciclaggio riferiti a tale oggetto non costituiscano condotte costituenti il reato presupposto[727]. Oggetto del reato di riciclaggio,

---

[720] GRZYWOTZ J., *Virtuelle Kryptowährungen und Geldwasche*, Berlin, 2019, p. 203 s.; NEUHAUSER S., *§ 261 StGB*, cit., Rn. 31
[721] Così GRZYWOTZ J., *Virtuelle kryptowahrungen und Geldwäsche*, cit., p. 228,.
[722] MAUME P., MAUTE L., FROMBERGER M., *Rechtsandbuch Kryptowerte*, cit., s. 568.
[723] BT-Dr. 19/24180.
[724] HERZOG F., *Bitcoins und Geldwäsche: Bestandsaufnahme strafrechtlicher Fallgestaltungen und regulatorischer Ansätze*, in *StV*, 2019, n. 6, p. 412 ss., p. 413 s.
[725] ARÁNGUEZ SÁNCHEZ C., *El Delito de Blanqueo de Capitales*, cit., p. 182;
[726] ABEL SOUTO M., *El delito de blanqueo en el Código penal español*, cit., p. 183.
[727] ABEL SOUTO M., *El delito de blanqueo en el Código penal español*, cit., p. 167; BLANCO CORDERO I., *El Delito de Blanqueo de Capitales*, cit., p. 349; ARÁNGUEZ SÁNCHEZ C., *El Delito de Blanqueo de*

dunque, possono essere i proventi ottenuti dalla commissione del reato presupposto, dunque il profitto del reato nonché i beni prodotti a seguito della commissione del reato[728]. Non appaiono dunque esservi ostacoli nel ritenere che oggetto del reato di riciclaggio possano essere anche le criptovalute, essendo queste economicamente valutabili.

8.3. L'elemento soggettivo

Per quanto riguarda l'elemento soggettivo, nel § 261 StGB è costituito dal dolo, che può essere anche eventuale[729]. Il dolo deve ricadere sull'oggetto del reato, la sua origine in un reato presupposto, l'atto di commettere il reato e il risultato del reato, per cui è necessario che l'autore del reato abbia almeno accettato che l'oggetto provenga da un qualche reato presupposto[730]. Tuttavia, a tal scopo è sufficiente che il reo si sia rappresentato la possibilità che l'oggetto in questione fosse provento di reato. Stessa cosa si può affermare per l'art. 301 *Código penal*: elemento soggettivo è il dolo, che può essere anche eventuale[731]. Anche in questo caso si esclude sia necessaria una conoscenza esatta e precisa in merito al reato presupposto, ma si ritiene sufficiente la consapevolezza dell'anormalità dell'operazione che si sta realizzando.

Il § 261 StGB punisce poi all' Abs. 6 anche il *leichtfertige Geldwäsche*, ovvero il riciclaggio colposo[732]. Questo reato è stato introdotto per colmare le lacune di punibilità dovute alle difficoltà di attribuzione e di prova, che però oggi sono parzialmente venute meno con l'eliminazione del catalogo dei reati presupposto. Ai fini della responsabilità penale è sufficiente che l'autore incautamente non riconosca che l'oggetto proviene da un qualsiasi reato, dato che a seguito della riforma qualsiasi reato è un possibile reato presupposto per il riciclaggio di denaro[733]. Nel progetto di legge ne era stata proposta l'eliminazione[734], ma ciò non è avvenuto. La dottrina, dunque, ha criticato duramente questa scelta, evidenziando che la punibilità del riciclaggio a titolo di colpa grave in combinazione

Capitales, cit., p. 205; CARPIO DELGADO J., *El delito de blanqueo de bienes en el nuevo Código penal*, Valencia, 1997, p. 102.

[728] CARPIO DELGADO J., *El delito de blanqueo de bienes en el nuevo Código penal*, cit., p. 98; ARÁNGUEZ SÁNCHEZ C., *El Delito de Blanqueo de Capitales*, cit., p. 204.

[729] RUHMANNSEDER F., *StGB § 261 Geldwäsche*, zit., Rn. 50

[730] *Ibid.*, Rn. 51.

[731] ALONSO PÉREZ F., *Delitos Contra el Patrimonio*, cit., p. 474.

[732] La *Leichtfertigkeit* tedesca non è altro che la colpa grave.

[733] EL-GHAZI M., LAUSTETTER C., *Das Gesetz zur Verbesserung*, cit., p. 214.

[734] RefE del BMJW, *Entwurf eines Gesetzes zur Verbesserung der strafrechtlichen Bekämpfung der Geldwäsche*, s. 19, disponibile *online* all'indirizzo https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RefE_Geldwaesche_Bekaempfung.pdf;jsessionid=D4103BD252AA5E4E0A39773F6545D1F5.2_cid324?__blob=publicationFile&v=2

con l'approccio *all-crime* comporta il rischio di una ipercriminalizzazione e di sovraccarico per il sistema giudiziario[735]. Nel tentativo di limitare la portata della norma, alcuni autori ritengono che a seguito dell'ultima riforma di cui al 2021 la nuova formulazione dei reati non sia compatibile con la punibilità del riciclaggio a titolo di colpa. A tal fine, evidenziano che l'Abs. 1 par. 1 n. 1 e 2, nonché l'Abs. 2 del § 261 richiedono tutti una certa "tendenza alla manipolazione" da parte del reo, difficilmente concepibile nel caso di una commissione meramente colposa[736].

Anche nell'ordinamento spagnolo il riciclaggio è punito a titolo di colpa grave (*blanqueo imprudente*), come previsto dall'art. 301.3 c.p. Alcuni autori ritengono però che la sanzione del riciclaggio a titolo di colpa sia in realtà in contrasto con la natura dolosa del reato in questione. Nonostante ciò, la giurisprudenza ritiene che il principio di legalità obblighi a ritenere il reato in questione punibile anche a titolo di colpa, per cui non si richiede più l'elemento soggettivo della conoscenza, ma la colpa grave[737].

Per altri autori la punibilità a titolo di colpa grave è possibile solo per le condotte di cui all'art. 301.2, perché quelle di cui al co. 1 sono compatibili unicamente con la modalità dolosa[738]. Per cui si ritiene possano essere chiamati a rispondere a titolo di colpa solo i soggetti che in virtù della *Ley* n. 10 del 28 aprile 2010 relativa alla prevenzione del riciclaggio e del finanziamento del terrorismo (*Ley de Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo*), sono obbligati ai relativi adempimenti ivi previsti[739]. Tuttavia, non manca chi evidenzia che in realtà la norma non distingue tra possibili soggetti attivi, per cui il riciclaggio colposo è reato comune e chiunque può essere sanzionato a titolo di colpa[740]. La giurisprudenza aderisce a tale ultima tesi, evidenziando che in linea di principio chiunque può essere punito per il riciclaggio a titolo di colpa[741]. In questo caso,

---

[735] GAZEAS N., *Das neue Geldwäsche-Strafrecht*, cit., p. 1044; EL-GHAZI M., LAUSTETTER C., *Das Gesetz zur Verbesserung der strafrechtlichen Bekämpfung der Geldwäsche*, cit., p. 213 s.
[736] ALTENHAIN K., FLECKENSTEIN L., *Der Gesetzentwurf zur Neufassung des § 261 StGB*, cit., p. 1050.
[737] V. Tribunal Supremo, sez. I, sentenza 16 aprile 2009, n. 790, evidenzia che «*la modalidad imprudente establecida en el art. 301.3 del CP contrasta con la naturaleza dolosa del delito de blanqueo […]. A pesar de ello, recuerda la doctrina que el principio de legalidad, evidentemente, obliga a considerar la comisión imprudente del delito. La imprudencia se exige que sea grave, es decir, temeraria. Así, en el tipo subjetivo se sustituye el elemento intelectivo del conocimiento, por el subjetivo de la imprudencia grave, que por ello recae precisamente sobre aquel elemento intelectivo*».
[738] MUÑOZ CONDE F., *Derecho Penal*, cit., p. 558.
[739] MUÑOZ CONDE F., *Derecho Penal*, cit., p. 558; ALONSO PÉREZ F., *Delitos Contra el Patrimonio*, cit., p. 480.
[740] BLANCO CORDERO I., *El Delito de Blanqueo de Capitales*, cit., p. 898; CALDERÓN CEREZO A., CHOCLÁN MONTALVO J.A., *Manual de Derecho Penal*, cit., p. 318. Tuttavia, in quest'ultimo caso gli stessi autori specificano che tale reato può essere commesso solo da quei soggetti che sono titolari di un dovere di diligenza ai sensi della legge o comunque di un regolamento.
[741] Tribunal Supremo, sez. I penale, sentenza 16 aprile 2009, n. 790.

però, il problema maggiore è determinare quale siano le dovute cautele nelle attività sociali dove non vi sono regole di condotta scritte[742]. In ogni caso, si evidenzia che la colpa dev'essere grave, quindi equivalente alla massima omissione della dovuta diligenza[743], ovvero al mancato rispetto dei più elementari criteri di cautela[744].

Con riferimento all'elemento soggettivo, dunque, le due fattispecie esaminate differiscono sensibilmente dalle corrispondenti norme italiane, che non ammettono la punibilità del riciclaggio a titolo di colpa.

8.4. La punibilità dell'autoriciclaggio

Il § 261 StGB è un reato comune, che può essere commesso da chiunque[745]. Tuttavia, qualora il reo sia l'autore del reato presupposto, quest'ultimo sarà punibile ai sensi degli Abs. da 1 a 6 solo se mette in circolazione l'oggetto nascondendone l'origine illecita. Ad oggi, dunque, nell'ordinamento tedesco persiste il c.d. privilegio dell'autoriciclaggio[746]. La legge tedesca, però, non sembra soddisfare i requisiti della direttiva 2018/1673/UE, che all'art. 3 par. 5 richiede agli Stati membri di rendere punibili alcuni atti di riciclaggio posti in essere dall'autore del reato presupposto, ovvero almeno lo scambio, il trasferimento nonché l'occultamento e la dissimulazione della vera natura dell'oggetto incriminato. È evidente che il § 261 Abs. 7 StGB non copre chiaramente tutti i reati previsti dalla direttiva[747]. Tuttavia, alcuni autori, alla luce del *considerando* n. 11 della direttiva[748], non vedono alcun conflitto tra il nuovo Abs. 7 e l'art. 3, par. 5 della direttiva[749].

La legge per il miglioramento del diritto penale contro il riciclaggio di denaro del 2021 ha mantenuto invariata nei contenuti la fondamentale impunità dell'autoriciclaggio[750].

---

[742] CABEDO VILLAMÓN F., ORTIZ NAVARRO J.F., AGUADO LÓPEZ S., *Conductas típicas y prueba electrónica en los fraudes electrónicos*, in C. Sanchis Crespo, *Fraude electrónico. Panorámica actual y medios jurídicos para combatirlo*, Cizur Menor, 2013, p. 241 ss., p. 303.
[743] ALONSO PÉREZ F., *Delitos Contra el Patrimonio*, cit., p. 480.
[744] BAJO FERNÁNDEZ M., BACIGALUPO SAGGESE S., *Derecho penal económico*, cit., p. 737.
[745] NESTLER N., *Bank- und Kapitalmarktstrafrecht*, cit., p. 357.
[746] TEXEIRA A., *Die Strafbarkeit der Selbstgeldwäsche*, in *NStZ*, 2018, p. 634 ss., p. 636.
[747] EL-GHAZI M., LAUSTETTER C., *Das Gesetz zur Verbesserung der strafrechtlichen Bekämpfung der Geldwäsche*, cit., p. 214.
[748] «*Gli Stati membri dovrebbero assicurare che taluni tipi di attività di riciclaggio siano perseguibili anche quando sono commessi dall'autore dell'attività criminosa che ha generato i beni («autoriciclaggio»). In tali casi, laddove l'attività di riciclaggio non si limiti alla mera detenzione o utilizzazione di beni, ma ne implichi anche il trasferimento, la conversione, l'occultamento o la dissimulazione, da cui derivi un danno supplementare oltre a quello già causato dall'attività criminosa, ad esempio mettendo in circolazione beni derivanti da un'attività criminosa e, così facendo, occultandone l'origine illecita, tale attività di riciclaggio dovrebbe essere perseguibile*».
[749] SCHRÖDER C., BLAUE A., *Die erste Richtlinie über die strafrechtliche Bekämpfung der Geldwäsche-Auswirkungen in Deutschland*, in *NZWiSt*, 2019, p. 161 ss., p. 165.
[750] GAZEAS N., *Das neue Geldwäsche-Strafrecht*, zit., s. 1043.

Tuttavia, va evidenziato che a seguito della modifica dell'Abs. 1 del § 261 STGB la disciplina dell'autoriciclaggio si discosta ora dal reato di riciclaggio, poiché quest'ultimo non punisce più l'effettivo "occultamento dell'origine", ma è sufficiente l'intenzione di ostacolare le indagini sull'origine (Abs. 1 S. 1 Nr. 1) o il nascondere un fatto che potrebbe essere importante per queste indagini (Abs. 2)[751]. Dunque, come avviene per gli artt. 648-*bis* e 648-*ter*.1 c.p., anche nell'ordinamento tedesco le condotte sanzionate a titolo di riciclaggio ed autoriciclaggio coincidono solo in parte. Per quanto riguarda la condotta di messa in circolazione, ci si deve riferire definizione del § 146 StGB, che punisce la contraffazione di moneta (*Geldfälschung*). Dunque, nell'intenzione del legislatore devono essere incriminati tutti quegli atti con i quali l'autore del reato rinuncia al suo effettivo potere di disposizione sull'oggetto provento di illeciti e coi quali un terzo acquisisce l'effettivo potere di disposizione sull'oggetto. Quale esempio di messa in circolazione del contante la relazione esplicativa della legge menziona anche il deposito di denaro contante ottenuto illegalmente su un conto bancario[752]. Ciò vale anche per i pagamenti su conti bancari detenuti dall'autore del reato a scopo esclusivamente personale[753].

L'applicazione dell'Abs. 7 §261 StGB è indipendente dalla condanna o dall'estinzione del reato presupposto[754], ma, naturalmente, trova senz'altro applicazione in caso di condanna per il reato presupposto[755].

Anche nell'ordinamento spagnolo il riciclaggio è un reato comune[756]. Infatti, l'art. 301 *Código penal* non richiede espressamente che il soggetto attivo del reato sia diverso dagli autori o partecipi. Anzi, a seguito della modifica di cui alla *Ley Orgánica* 5/2010 è stato aggiunto l'inciso "da lui commessa o da qualsiasi altra persona" accanto ad "attività delittiva", per cui oggi la norma ammette espressamente che anche sia l'autore che il partecipe nel reato presupposto possano rispondere del reato di riciclaggio, mettendo così

[751] ALTENHAIN K., FLECKENSTEIN L., *Der Gesetzentwurf zur Neufassung des § 261 StGB,* cit., p. 1051.
[752] Vgl. BT-Drs. 18/6389, p. 14.
[753] TEXEIRA A., *Die Strafbarkeit der Selbstgeldwäsche,* cit., p. 639; BGH, ordinanza 27 novembre 2018 – 5 StR 234/18.
[754] BGH, sentenza 20 settembre 2000 - 5 StR 252/00.
[755] BGH, ordinanza 16 agosto 2016 – 5 StR 182/16; BGH, ordinanza 8 maggio 2017 – GSSt 1/17.
[756] DE LA CUESTA ARZAMENDI J.L., *Tendencias normativas en la lucha contra el blanqueo*, in F. Jiménez García (dir.), J. Ropero Carrasco (dir.), A. Pastor Palomar (coord.), *Blanqueo de capitales y corrupción. Interacciones para su erradicación desde el derecho internacional y los sistemas nacionales*, Cizur Menor, 2017, p. 51 ss., p. 62.

fine al dibattito esistente sul punto[757]. Dunque si ritiene che in questo caso vi sarà concorso di reati tra il riciclaggio e il reato presupposto[758].

La punibilità dell'autoriciclaggio è stata oggetto di critiche, in particolare con riferimento alle condotte che fondamentalmente consistono in un mero godimento dei beni (possesso e utilizzo), dato che la punibilità di queste ultime anche a titolo di riciclaggio per l'autore del reato presupposto può comportare la violazione del principio costituzionale del *ne bis in idem*[759]. Pertanto, in mancanza di una clausola limitativa della responsabilità penale per il concorrente nel reato presupposto simile a quelle presenti in Italia e Germania, la giurisprudenza spagnola ha cercato di limitare la portata applicativa dell'art. 301 c.p., in modo da evitare di infliggere pene sproporzionate. Pertanto, ha escluso l'applicabilità della norma in esame nei casi più lievi[760] e, soprattutto, in quei casi in cui le condotte sono inadeguate ad assicurare l'inserimento dei beni di provenienza illecita nel traffico economico[761]. In particolare, si evidenzia che il semplice possesso è condotta che già integra il reato presupposto, con conseguente inapplicabilità dell'art. 301 c.p.[762].

Sia la fattispecie tedesca che quella spagnola prendono espressamente in considerazione l'ipotesi che il reato presupposto del riciclaggio sia stato commesso all'estero, cosa che, invece, le fattispecie italiane in materia non fanno. L'Abs. 9 del § 261 StGB, infatti, specifica che oggetto del reato di riciclaggio ai sensi della normativa tedesca possono essere anche i proventi di un reato commesso all'estero, se questo costituisce reato ai sensi della legge tedesca ed è punibile nel luogo in cui è stato commesso il reato, oppure è punibile ai sensi di una delle disposizioni e convenzioni dell'Unione europea elencate, tra le quali, tuttavia, non sono ricomprese quelle in materia di frodi e falsificazioni di strumenti

---

[757] FARALDO CABANA P., *Antes y después de la tipificación expresa del autoblanqueo de capitales*, in *Estudios Penales y Criminológicos*, 2014, n. 34, p. 41 ss., p. 56.

[758] ALONSO PÉREZ F., *Delitos Contra el Patrimonio*, cit., p. 472 e BLANCO CORDERO I., *El Delito de Blanqueo de Capitales*, cit., p. 670. In giurisprudenza v. Tribunal Supremo, sez. I penale, sentenza 31 marzo 2010, n. 309, secondo cui il reato presupposto è indipendente rispetto al riciclaggio, per cui l'autore del primo può essere autore anche del secondo.

[759] BLANCO CORDERO I., *Estrategia penal contra las ganancias de la corrupción: blanqueo de capitales, delito fiscal y enriquecimiento ilícito*, in *Blanqueo de capitales y corrupción. Interacciones para su erradicación desde el derecho internacional y los sistemas nacionales*, cit., p. 27 ss., p. 37.

[760] Tribunal Supremo, sez. I penale, sentenza 26 novembre 2014, n. 849.

[761] Tribunal Supremo, sez. II penale, sentenza 29 aprile 2015, n. 265, secondo cui «*el art 301 CP solo tipifica una modalidad de conducta que consiste en realizar actos encaminados en todo caso a ocultar o encubrir bienes de procedencia delictiva, o a ayudar al autor de esta actividad a eludir la sanción correspondiente. Con esta interpretación, más restrictiva, evitamos excesos, como los de sancionar por autoblanqueo al responsable de la actividad delictiva antecedente, por el mero hecho de adquirir los bienes que son consecuencia necesaria e inmediata de la realización de su delito*».

[762] Tribunal Supremo, sez. II penale, sentenza 29 marzo 2016, n. 238, che però ha condannato ugualmente gli imputati per riciclaggio evidenziando che l'intestazione a prestanome dei beni di provenienza illecita non costituisce mero possesso, ma è condotta diretta a nascondere la vera origine dei beni in questione.

di pagamento diversi dai contanti o in materia di attacchi ai sistemi di informazione. La norma, dunque, richiede il requisito della doppia incriminazione, tranne che nei casi in cui l'attività delittuosa sia una di quelle indicate nei provvedimenti dell'Unione Europea di cui all'Abs. 9, n. 2 § 261 StGB[763]. Si evidenzia, però, che la direttiva 2018/1673/UE sulla lotta al riciclaggio del denaro tramite il diritto penale obbliga gli Stati membri a punire il riciclaggio prescindendo dalla presenza della doppia incriminazione del reato presupposto per una lunga serie di attività criminose, tra cui la truffa e la criminalità informatica. Pertanto, la normativa tedesca non è pienamente conforme alle disposizioni europee.

L'art. 301.4 *Código penal*, invece, in maniera molto più semplice e lineare, specifica che l'autore del reato è punibile anche se il reato presupposto è stato commesso all'estero o se le condotte di riciclaggio sono state commesse in tutto o in parte all'estero. Anche se dal tenore letterale della norma appare indifferente che il reato presupposto sia o meno sanzionato all'estero, vi è chi ritiene che si applichi comunque il principio di doppia incriminazione, per cui il reato presupposto deve costituire reato in entrambi i Paesi, anche se non è necessaria la perfetta coincidenza delle norme giuridiche[764].

9. La responsabilità penale dei *financial manager*

Come esaminato nel capitolo precedente (v. *supra*, cap. IV, par. 4), nella maggior parte dei casi i *financial manager* (*Finanzagenten* o *muleros*) non sono che privati cittadini, ma a volte possono essere dipendenti dell'istituto di credito. Per reprimere tale fenomeno, anche in Germania e in Spagna le banche e le altre società di servizi finanziari sono incluse nella cerchia dei soggetti obbligati dalla legge sul riciclaggio di denaro. In Germania, essi sono elencati tra i soggetti cui di applica la normativa antiriciclaggio ai sensi del § 2 Abs. 1 della legge sul riciclaggio (*Geldwäschegesetz* -GwG), per cui sono obbligati ad identificare tutti i loro nuovi clienti. La violazione di quest'obbligo è punita con un illecito amministrativo (§ 56 GwG). Anche il § 25h della legge bancaria tedesca (*Kreditwesengesetzes* - KWG) e della legge tedesca sulla vigilanza delle assicurazioni (*Versicherungsaufsichtsgesetzes* - VAG) descrivono in dettaglio le misure di salvaguardia da adottare, le responsabilità e i doveri dei destinatari della KGW e della VAG per prevenire e combattere il riciclaggio di denaro. Anche in Spagna l'art. 2 della *Ley* n. 10 del 28 aprile 2010 relativa alla prevenzione del riciclaggio e del finanziamento del terrorismo include,

[763] NESTLER N., *Strafanwendungsrechtliche Probleme des reformierten Geldwäschetatbestands (Teil 2)*, in *JA*, 2022, n. 7, p. 814 ss., p. 820.
[764] BLANCO CORDERO I., *El Delito de Blanqueo de Capitales*, cit., p. 391.

oltre agli istituti di credito, coloro che si dedicano professionalmente all'intermediazione nella concessione di prestiti e crediti tra gli obbligati al rispetto di una serie di obblighi antiriciclaggio, che spaziano dall'identificazione del cliente all'obbligo di informare determinati organismi in caso di operazioni sospette[765].

In Germania, in linea di principio la responsabilità penale di un agente finanziario viene presa in considerazione a titolo di partecipazione (*Teilnahme*) nella precedente frode informatica del *phisher* o a titolo di riciclaggio di denaro in relazione ai beni ottenuti dalla frode informatica. Normalmente, il *financial manager* non è al corrente della commissione del reato presupposto e i suoi atti si limitano alla trasmissione dei beni ricevuti sul suo conto. La frode informatica è consumata quando l'autore ha conseguito il profitto, dunque, nel caso del *phishing* e delle *Advance fee fraud*, non appena il denaro della vittima viene accreditato sul conto corrente[766]. Per questo motivo, nella maggior parte dei casi i *financial manager* sono stati condannati a titolo di riciclaggio di denaro[767]. La gestione da parte di quest'ultimo della somma di denaro trasferita sul suo conto (tenere il denaro pronto, ritirarlo, trasferirlo in contanti) può integrare tutte le condotte di riciclaggio di denaro descritte nel § 261 Abs. 1 e 2 StGB[768]. Se l'agente finanziario ritira i fondi che la vittima gli ha direttamente inviato sul suo conto e li trasferisce al *phisher* dopo aver dedotto la sua commissione, è ipotizzabile anche una responsabilità penale per concorso a titolo di complicità (*Beihilfe*) in frode informatica. Prima del ritiro del denaro il § 261 StGB non può considerarsi commesso: quando il conto viene aperto e i dettagli del conto vengono comunicati all'autore del reato presupposto non esiste ancora alcun oggetto, di conseguenza non viene coperta alcuna traccia cartacea o viene messo a rischio un ritrovamento o un sequestro. Ciò vale anche qualora il bonifico venga effettuato e accreditato dalla vittima sul conto dell'agente finanziario. In tal caso l'agente finanziario è responsabile esclusivamente a titolo di concorso nel reato presupposto[769]. Alcuni autori sostengono che, oggettivamente, la fornitura dei dati del conto da parte del *financial manager* allo scopo di ivi far addebitare il denaro provento di frode informatica costituisca un atto di complicità riconducibile alla condotta di ausilio. Infatti, la consegna dei dati del conto corrente rende possibile il reato, per cui si configura

[765] DE LA CUESTA ARZAMENDI J.L., *Tendencias normativas en la lucha contra el blanqueo*, cit., p. 65.
[766] KOCHHEIM D., *Cybercrime und Strafrecht*, zit., s. 529 ff.
[767] BGH, ordinanza 28 febbraio 2013 – 2 Ars 91/13.
[768] NEUHEUSER S., *Die Strafbarkeit des Bereithaltens und Weiterleitens des durch „Phishing" erlangten Geldes*, in *NStZ*, 2008, p. 492 ss., p. 496.
[769] ALTEHAIN K., *StGB § 261 Geldwäsche; Verschleierung unrechtmäßig erlangter Vermögenswerte*, Kindhäuser/Neumann/Paeffgen, Strafgesetzbuch, 5. Auflage 2017, Rn. 130b

un'assistenza oggettiva al reato ai sensi del § 27 StGB[770]. In alcune sentenze, il BGH ha sostenuto che la partecipazione dell'agente finanziario lo rende sostanzialmente un complice del reato presupposto di frode informatica[771]. Tuttavia, sorge un problema per quanto riguarda il doppio dolo di partecipazione, poiché il complice è punibile ai sensi del § 27 Abs. 1 StGB solo se agisce con coscienza e volontà di concorrere nella commissione di un reato[772]. In molti casi, tuttavia, non si sarà in grado di dimostrare il doppio dolo richiesto dal § 27 StGB, perché il *financial manager* o viene ingannato dal phisher o comunque viene lasciato all'oscuro rispetto alle sue vere intenzioni. La semplice conoscenza o presunzione che il denaro provenga da un reato, infatti, non è però sufficiente ai fini del dolo di partecipazione. Nei casi in cui l'agente finanziario ipotizza la commissione di un altro reato presupposto diverso rispetto a quello commesso, la sua condotta costituisce un mero tentativo di partecipazione a titolo di favoreggiamento nel reato principale, dunque non è punibile[773].

In questo contesto si distingue anche tra complicità in frode informatica (§§ 263a, 27 StGB) e favoreggiamento (§ 257 StGB). Infatti, tra l'accredito e il trasferimento al *phisher* l'illecito profitto può ancora essere stornato e la persona offesa può ancora disporre del denaro bloccandone l'invio, per cui è possibile ipotizzare che un terzo, ovvero il *financial manager*, intervenga in aiuto del reo per assicurare che il trasferimento del denaro vada a buon fine. Fino alla consumazione del reato presupposto, la complicità è possibile e per la giurisprudenza dev'essere contestato in via preferenziale[774]. Per quanto riguarda i presupposti del favoreggiamento come reato successivo alla frode informatica, la giurisprudenza del BGH ha sostenuto che il favoreggiamento è punibile solo nella misura in cui l'autore del reato presupposto si assicuri in tal modo i vantaggi diretti del reato, che deve ricevere solo dopo aver compiuto l'atto di favoreggiamento[775]. Il § 257 StGB, dunque, può trovare applicazione in un numero piuttosto limitato di casi. Se la refurtiva viene inizialmente depositata sul conto dell'agente e viene da lui inoltrata solo dopo un certo lasso di tempo, allora l'agente fornisce assistenza all'autore del reato presupposto al fine di

[770] SEIDL A., FUCKS K., *Die Strafbarkeit des Phishing nach Inkrafttreten des 41. Strafrechtsänderungsgesetzes*, in *HRRS*, 2010, n. 2, p. 85 ss., p. 90.
[771] BGH, ordinanza 11 settembre 2014 – 4 StR 312/14: "*Von der materiellen Beendigung einer Tat des Computerbetruges i. S. von § 263 a StGB, bei der auf Grund einer Manipulation von Datenverarbeitungsvorgängen ein Geldbetrag vom Konto des Gesch. auf ein Empfängerkonto geleitet wird, ist erst auszugehen, wenn entweder das überwiesene Geld vom Empfängerkonto abgehoben oder auf ein zweites Konto weiterüberwiesen worden ist*". Così anche BGH, ordinanza 28 febbraio 2012 – 3 StR 435/11.
[772] GROPP W., SINN A., *Strafrecht AT*, zit., s.480.
[773] NEUHEUSER S., *Die Strafbarkeit des Bereithaltens,* cit., p. 494; SEIDL A., FUCKS K., *Die Strafbarkeit des Phishing,* cit., p. 90.
[774] BGH, ordinanza 11 settembre 2014 – 4 StR 312/14.
[775] BGH, ordinanza 11 aprile 2013 – 2 StR 406/12.

assicurargli i benefici del reato (§ 257 Abs. 1 StGB). In questo caso, dunque, commette favoreggiamento e sarà sanzionato con la stessa pena prevista per il reato base (§ 257 Abs. 2 StGB)[776].

Non è facile distinguere i casi in cui il *financial manager* agisce come concorrente nel reato presupposto, a titolo di favoreggiamento ai sensi del § 257 StGB o riciclaggio ex § 261 StGB. Questo perché la stessa giurisprudenza del BGH è ambigua in merito all'identificazione del momento esatto in cui si verifica la consumazione di una frode informatica. La dottrina, pertanto, tenta di risolvere il problema sostenendo che la scelta del titolo del reato debba effettuata sulla base dell'elemento soggettivo. Sebbene il *financial manager* compia sempre la stessa azione in tutti i casi, ovvero inoltrare i pagamenti ricevuti sul suo conto bancario, il titolo di reato viene determinato sulla base della loro "vicinanza" al reato presupposto. Dunque, i *financial manager* di primo (§§ 263a, 27 StGB) e secondo (§ 257 StGB) grado agiscono sostanzialmente nello stesso modo, ma vengono distinti a seconda della presenza o meno del dolo di favoreggiamento. Pertanto, i soggetti che agiscono solo dopo la consumazione della frode informatica commettono favoreggiamento (§ 257 StGB) o riciclaggio di denaro (§ 261 StGB), se partecipano all'occultamento dei flussi di pagamento o dei canali di vendita[777].

Qualora si qualifichi la condotta del *financial manager* come riciclaggio di denaro, sorge il problema dell'individuazione dell'elemento soggettivo del reato, poiché è necessario stabilire in che misura tale soggetto sia coinvolto nel reato presupposto e quale sia la sua conoscenza di quest'ultimo. Come sopra evidenziato, il riciclaggio di denaro in Germania è punibile anche a titolo di colpa grave. Dunque, il *financial manager* può essere punito ai sensi del § 261 Abs. 6 StGB per riciclaggio di denaro a titolo di colpa se incautamente non riconosce che denaro da lui trasferito è provento di una frode informatica o di un altro reato presupposto. A tal proposito, la giurisprudenza del BGH ha affermato che la colpa grave presuppone che l'origine delittuosa del bene sia evidente sulla base delle circostanze fattuali del caso concreto e che l'autore del reato abbia deciso di agire comunque per particolare indifferenza o grave disattenzione[778].

Resta ora da esaminare se il *phisher* e il *financial manager* concorrente nel reato presupposto possano essere entrambi puniti a titolo di riciclaggio di denaro. La punibilità del riciclaggio di denaro commesso dall'autore o dai partecipanti al reato presupposto richiede

[776] KOCHHEIM D., *Cybercrime und Strafrecht*, cit., p. 530.
[777] *Ibid*.
[778] BGH, ordinanza 11 settembre 2014 – 4 StR 312/14, zit.

la presenza congiunta di due condizioni, ovvero la messa in circolazione e l'occultamento dell'origine illecita dell'oggetto[779]. Di conseguenza, gli atti "interni" tra coautori, come i trasferimenti successivi tra i conti degli stessi autori, non rientrano nel concetto di messa in circolazione[780]. Come la condotta di occultamento, con "occultamento della provenienza" (*Verschleiern der Herkunft*) si indica il comportamento manipolativo, clandestino e quindi gli atti tipici e centrali del riciclaggio che vanno oltre l'ordinaria gestione del bene provento del reato. Qualora il reo non utilizzi artifici ingannevoli, le condotte di ostacolo, messa in pericolo dell'identificazione dell'origine, di ritrovamento, ecc. non sono ricomprese nella nozione di "occultamento". Come si evince dalla formulazione della norma, quando l'autore del reato di autoriciclaggio mette in circolazione il bene provento di reato, deve allo stesso tempo nasconderne l'origine illecita. L'autoriciclaggio, dunque, è punibile solo qualora la condotta di messa in circolazione sul mercato coincida con quella di occultamento[781]. Pertanto, qualora *phisher* e *financial manager* trasferiscono il denaro esclusivamente tra i conti correnti di cui sono titolari si applica la clausola di non punibilità di cui al § 261 Abs. 7 StGB, data l'assenza dell'inganno.

Anche nell'ordinamento spagnolo si registrano delle difficoltà nell'individuazione della responsabilità penale dei *financial manager*, ovvero i c.d. *muleros*. La determinazione del titolo di reato cui il *mulero* può essere chiamato a rispondere dipende dal momento in cui si considera consumato il reato di frode informatica, perché quest'ultimo può essere punito a titolo di concorso nel reato solo se quest'ultimo non si è ancora consumato[782]. L'orientamento giurisprudenziale maggioritario ritiene che gli stessi debbano rispondere del delitto di frode informatica a titolo di concorso, quali *cooperadores necesarios*, poiché il loro operato funge da *conditio sine qua non* per la consumazione della frode informatica perpetrata dall'autore e lo fanno in accordo con l'autore del reato[783]. In particolare, si evidenzia che il *financial manager* interviene prima della consumazione del reato di frode informatica, perché è con il trasferimento del denaro, che viene effettuato sul conto del *financial manager*, che la frode informatica si consuma. Pertanto, la commissione di tale reato non sarebbe stata possibile se quest'ultimo non avesse messo a disposizione del *phisher*

[779] TEIXEIRA A., *Die Strafbarkeit der Selbstgeldwäsche*, cit., p. 635.
[780] NEUHEUSER S., *Die begrenzte Straflosigkeit der Selbstgeldwäsche (§ 261 Abs. 9 S. 2 und 3 StGB)*, in *NZWiSt*, 2016, p. 265 ss., p. 266.
[781] *Ibid.*, p. 267.
[782] CABEDO VILLAMÓN F., ORTIZ NAVARRO J.F., AGUADO LÓPEZ S., *Conductas típicas y prueba electrónica en los fraudes electrónicos*, cit., p. 290.
[783] Tribunal Supremo, sez. I penale, sentenza 12 giugno 2007, n. 3935; Tribunal Supremo, sez. I penale, sentenza 3 febbraio 2009, n. 3926; Tribunal Supremo, sez. I penale, sentenza 16 marzo 2009, n. 556.

il suo conto corrente, perché per la consumazione della frode informatica non è sufficiente disporre delle credenziali del conto corrente *online* della vittima, ma è necessario anche il possesso di un conto corrente sul quale si possa depositare il denaro di quest'ultima, in modo tale da ottenere il beneficio economico. Va evidenziato, però, che la responsabilità a titolo di concorso in frode informatica è ipotizzabile solo per il primo *financial manager*, ovvero quello che riceve il denaro direttamente dalla vittima, non per gli altri che eventualmente intervengono successivamente per disperdere le tracce del denaro, perché questi ultimi intervengono quando la frode informatica è già consumata.

Altro punto di fondamentale importanza è la determinazione del grado di conoscenza del *financial manager* in merito alla commissione della frode informatica. Per quanto riguarda l'elemento soggettivo, infatti, si ricorda che la frode informatica richiede il dolo specifico. Pertanto, è necessario che il *financial manager* sia a conoscenza del fatto di star partecipando alla commissione di un reato di frode informatica, che agisca al fine di trarre un ingiusto profitto e sia a conoscenza dell'origine illegale del denaro[784]. Per questo motivo, in alcuni casi la giurisprudenza ha escluso la responsabilità penale dei *financial manager* qualora gli stessi non siano consapevoli che il denaro loro inviato sia stato sottratto fraudolentemente ad un terzo[785]. In altri casi, però, la giurisprudenza ha comunque sanzionato i *financial manager* privi di tale consapevolezza per frode informatica, ritenendo che quest'ultima fattispecie possa essere punita anche a titolo di dolo eventuale[786]. A tal proposito, si ritiene che l'apertura di un nuovo conto corrente da parte del *financial manager* appositamente per farvi transitare le somme inviategli dal *phisher* possa costituire un rilevante indizio in merito alla sussistenza del dolo di partecipazione[787].

Tuttavia, come sopra evidenziato, la qualificazione della condotta dei *muleros* a titolo di concorso nel reato di frode informatica non è affatto pacifica. Alcuni autori, infatti, sostengono che punire il *financial manager* con la medesima pena prevista per il *phisher* sia contrario al principio di proporzione, dato che il primo rappresenta l'"anello debole" della catena del *phishing* e interviene solo nell'ultima fase, peraltro senza che la sua attività

[784] CABEDO VILLAMÓN F., ORTIZ NAVARRO J.F., AGUADO LÓPEZ S., *Conductas típicas y prueba electrónica*, cit., p. 294.
[785] Audiencia Provincial di Soria, sez. I, sentenza 27 febbraio 2012, n. 16.
[786] Cft. Tribunal Supremo, sez. I, sentenza 26 dicembre 2008, n. 953, che fa riferimento all' "*ignorancia deliberada*" del *mulero*, ritenendo sussistente il dolo eventuale qualora l'agente potendo e dovendo conoscere il fatto che l'agire in questione costituisce un illecito, decide di non informarsi e di prestare comunque la sua collaborazione.
[787] BREL PEDREÑO A., *La responsabilidad criminal y la tipificación de las conductas en el fraude electrónico*, in *Fraude electrónico*, cit., p. 21 ss., p. 32.

presupponga in ogni caso la piena conoscenza dell'illecita provenienza del denaro ricevuto[788].

Anche in questo caso vi è una parte della giurisprudenza che non ritiene configurabile la responsabilità dei *muleros* a titolo di concorso nel reato presupposto, evidenziando che quando tali soggetti intervengono il reato in questione è già consumato[789]. In particolare, viene evidenziato che i soggetti in questione non partecipano alla manipolazione informatica e che, invece, partecipano ad un'operazione successiva rispetto alla commissione della frode informatica, che già si è consumata nel momento in cui la vittima ha subìto una diminuzione patrimoniale a seguito della manipolazione informatica, consistente nell'occultare il denaro e trasferirlo in un luogo dal quale non può essere recuperato. Pertanto, una parte della giurisprudenza ha ritenuto il *financial manager* responsabile a titolo di riciclaggio[790]. Alcuni autori evidenziano che la riforma 2010, con l'ampliamento dell'ambito applicativo del reato di riciclaggio, ha reso possibile la punibilità dei *muleros* a titolo di riciclaggio, perché presupposto del riciclaggio oggi può essere qualsiasi "attività delittiva", non necessariamente un reato consumato, e, soprattutto, perché il *mulero* si limita a possedere e a trasmettere il denaro ricevuto sul conto[791]. Dunque, si ritiene che la condotta del *financial manager* che riceve sul conto corrente il denaro dalle vittime ed a sua volta lo trasferisca, sia qualificabile come possesso o acquisizione ai sensi dell'art. 301.1 c.p.[792].

Come sopra evidenziato, anche in Spagna il riciclaggio di denaro è punibile a titolo di colpa. La colpa del *financial manager* dev'essere grave, per cui occorre che quest'ultimo non abbia rispettato il dovere di cautela esigibile dall'uomo comune[793]. La colpa può essere cosciente o meno, per cui sussiste sia se il soggetto si rappresenta la provenienza illecita del denaro, sia se non se la rappresenta, ma poteva rappresentarsela in base all'esistenza di indizi che rivelano l'origine illegale del denaro[794]. La giurisprudenza ha ritenuto sussistente la colpa grave nei casi in cui il reo sia venuto meno all'osservanza del dovere di diligenza esigibile dall'uomo comune, infrangendo in modo grave le norme di precauzione, evidenziando che l'offerta di lavoro con la quale si offre al *financial manager* una

[788] VELASCO NÚÑEZ E., *Estafa informática y banda organizada. Phishing, pharming, smishing y «muleros»*, in *La ley penal*, 2008, n. 49, p. 1 ss., p. 8.
[789] Audiencia Provincial de Valladolid, sez. IV penale, sentenza 21 giugno 2010, n. 263.
[790] Tribunal Supremo, sez. I penale, sentenza 25 ottobre 2012, n. 834. Così anche Audiencia Provincial de Sevilla, sez. VII penale, sentenza 22 marzo 2012, n. 174; Audiencia Provincial de Gijón, sez. VIII penale, sentenza 11 settembre 2012, n. 148; Audiencia Provincial de Leon, sentenza 29 luglio 2011, n. 186.
[791] MIRÓ LLINARES F., *La respuesta penal al ciberfraude*, cit., p. 37.
[792] BLANCO CORDERO I., *El Delito de Blanqueo de Capitales*, cit., p. 862.
[793] CABEDO VILLAMÓN F., ORTIZ NAVARRO J.F., AGUADO LÓPEZ S., *Conductas típicas y prueba electrónica*, cit., p. 301.
[794] *Ibid*.

commissione per la semplice "messa a disposizione" di un conto corrente è certamente anomala e certamente mette in allarme qualsiasi persona di media conoscenza[795]. Nella maggior parte dei casi il *financial manager* è stato condannato per riciclaggio a titolo di colpa[796], ma non sono mancate pronunce di condanna a titolo di dolo[797]. In altri casi ancora, la giurisprudenza del *Tribunal Supremo* ha assolto il *financial manager* per insussistenza della colpa grave, evidenziando che può ritenersi che il reo abbia agito in modo temerario solo nel caso in cui sia dimostrato che il *ciudadano más descuidado* si sarebbe comportato in maniera diversa[798].

Per alcuni autori in realtà non vi è alcun contrasto giurisprudenziale in merito alla qualificazione della condotta del *financial manager*, poiché la soluzione deve necessariamente divergere in base alla conoscenza che ha l'autore della frode informatica: la loro responsabilità può essere a titolo di concorso nella frode informatica solo se hanno la piena coscienza e volontà di partecipare alla frode informatica[799].

Altra giurisprudenza, invece, ha escluso la possibilità di punire il *financial manager* a titolo di riciclaggio, perché quest'ultimo sanziona le condotte aventi ad oggetto i proventi dell'attività illecita, non l'oggetto del reato presupposto, mentre in questo caso il denaro costituisce oggetto materiale della frode informatica[800]. Tale affermazione, tuttavia, è in contrasto con la tesi maggioritaria, che ritiene che qualora l'oggetto del riciclaggio e l'oggetto materiale del reato presupposto coincidano, non vi è nessun ostacolo a considerare quest'ultimo oggetto idoneo del reato di riciclaggio[801]. Si evidenzia poi che oggetto materiale della frode informatica è, per l'appunto, il sistema informatico, non il denaro della vittima, che costituisce, invece, il profitto del reato.

Alcuni autori ritengono che in realtà il *financial manager* dovrebbe essere punito a titolo di ricettazione di cui all'art. 298 c.p., evidenziando che nella maggior parte dei casi quest'ultimo non è a conoscenza della previa commissione di una frode informatica e non è realmente un appartenente alle associazioni a delinquere dedite al *phishing* e che la pena

[795] Così Tribunal Supremo, sez. I, sentenza 16 aprile 2009, n. 790.
[796] Audiencia Provincial de Valladolid, sez. IV penale, sentenza 21 giugno 2010, n. 263; Audiencia Provincial de Granada, sez. II penle, sentenza 27 giugno 2008, n. 414; Audiencia Provincial de Huesca, sez. I penale, sentenza 31 maggio 2010, n. 89.
[797] Audiencia Provincial de Oviedo, sez. II penale, sentenza 29 novembre 2012, n. 556.
[798] Tribunal Supremo, sez. I penale, sentenza 19 dicembre 2014, n. 997; Tribunal Supremo, sez. I penale, sentenza 19 dicembre 2013, n. 997; Tribunal Supremo, sez. I penale, sentenza 25 settembre 2014, n. 615.
[799] MIRÓ LLINARES F., *La respuesta penal al ciberfraude*, cit., p. 42. A tal proposito si evidenzia che Tribunal Supremo, sez. I penale, sentenza 20 novembre 2015, n. 743 ha ritenuto il *financial manager* responsabile del reato di frode informatica analizzando unicamente la sussistenza del dolo in capo all'autore.
[800] Audiencia Provincial de Madrid, sez. VI penale, sentenza 26 maggio 2008, n. 271.
[801] BLANCO CORDERO I., *El Delito de Blanqueo de Capitales*, cit., p. 349.

prevista da quest'ultimo reato è maggiormente proporzionata al disvalore del fatto, dato che non partecipa alla commissione della frode informatica, bensì all'occultamento del profitto della stessa[802]. Per altri ancora, la condotta del *mulero* può essere ricondotta al diverso reato di favoreggiamento (*encubrimiento*) di cui all'art. 451 c.p.[803].

In entrambi gli ordinamenti, dunque, vi sono difficoltà nell'identificazione del titolo di reato per il quale possono essere chiamati a rispondere i *financial manager*. Tuttavia, a differenza di quanto avviene nell'ordinamento italiano, la presenza in entrambi gli ordinamenti del riciclaggio colposo consente di mitigare il trattamento sanzionatorio

10. Riflessioni conclusive

Dall'analisi effettuata emerge come le disposizioni in materia di reati cibernetici contro il patrimonio dell'ordinamento italiano, tedesco e spagnolo presentano tutte un nucleo comune. Questo è dovuto al fatto che si tratta comunque di disposizioni adottate sull'impulso di provvedimenti sovranazionali di vario genere. Tuttavia, a seguito del recepimento delle direttive 2013/40/UE e 2019/713/UE si può notare che vi è stato un disallineamento tra le stesse. Infatti, mentre prima dell'adozione della direttiva 2019/713/UE in materia di frodi e falsificazioni di strumenti diversi dai contanti, le disposizioni in materia di falsificazione di carte di credito erano piuttosto simili in tutti e tre i Paesi, ora vi sono divergenze anche significative. Basti pensare alle nuove fattispecie che puniscono gli atti preparatori alla commissione dell'indebito utilizzo e falsificazione degli strumenti diversi dai contanti (ovvero l'art. 493-*quater* c.p., il § 152c StGB e gli artt. 249.2 lett. b) e 400 código penal), ove vi sono tre diverse discipline per i tre diversi Paesi che o non hanno nulla in comune oppure sono soltanto vagamente simili. Questo è dovuto alla differente modalità di trasposizione della normativa europea da parte dei diversi legislatori. Infatti, il legislatore spagnolo, in modo simile al nostro, ha ritenuto di dover attuare entrambe le direttive riportando il contenuto di interi articoli nelle diverse fattispecie, senza preoccuparsi di verificare attentamente se le condotte menzionate nelle direttive fossero già sanzionate nell'ordinamento. Ciò, come si è esaminato, ha comportato un'incontrollata moltiplicazione di fattispecie penali dal contenuto quasi identico, la cui individuazione dei rapporti costituisce tutt'oggi questione spinosa e controversa. In questo la nostra legislazione in materia di reati cibernetici e quella spagnola si somigliano, anche se permangono alcune

[802] VELASCO NÚÑEZ E., *Estafa informática y banda organizada*, cit., p. 8.
[803] CABEDO VILLAMÓN F., ORTIZ NAVARRO J.F., AGUADO LÓPEZ S., *Conductas típicas y prueba electrónica*, cit., p. 305.

differenze. Al contrario, il legislatore tedesco ha ritenuto di dover modificare la propria normativa per adattarla alle menzionate direttive solo in minima parte, preferendo agire in modo autonomo ed estemporaneo, come dimostra l'introduzione della fattispecie di cui al § 127 StGB. Questo ha "allontanato" la legislazione tedesca in materia rispetto a quella italiana e spagnola. Diverso discorso, invece, va fatto per la disciplina penale in materia di riciclaggio. In quest'ultimo caso è stato il legislatore italiano a modificare solo in minima parte la propria normativa penale per adattarla alla normativa europea antiriciclaggio, senza, pertanto, aumentare esponenzialmente ed in modo eccessivo l'ambito applicativo delle fattispecie incriminatrici in materia, come invece hanno fatto il legislatore tedesco e spagnolo aumentando il numero delle condotte punibili. La presenza del riciclaggio colposo, però, consente di mitigare il trattamento sanzionatorio per i *financial manager*.

É certamente vero che l'armonizzazione in materia penale non coincide affatto con la totale identità delle norme[804], ma non si può negare che il fatto che in questo particolare ambito le modifiche effettuate alle fattispecie per "adeguarle" alla normativa europea abbiano avuto quale effetto quello di creare delle discrepanze tra le stesse e le norme europee ad esse assimilabili. Ciò è sicuramente contrario rispetto all'obiettivo perseguito dal legislatore europeo con l'adozione di tali provvedimenti ed è una stortura che è necessario correggere quanto prima. Nel prossimo capitolo, pertanto, si proporranno soluzioni per questo delicato problema, nonché per gli altri già individuati nei capitoli precedenti.

[804] HECKER B., *§ 10 Harmonisierung*, in U. Sieber, H. Satzger, B. Von Heintschel-Heinegg (a cura di), *Europäisches Strafrecht*, Baden-Baden, 2014, p. 272 ss., p. 273. V anche AMBOS K., *Internationales Strafrecht*, München, 2018, p. 441 in merito alla differenza tra armonizzazione ed assimilazione.

Capitolo VI

Conclusioni e prospettive *de jure condendo*

Sommario: 1. Considerazioni politico-criminali sul ricorso allo strumento penale per tutelare il patrimonio e sulla collocazione sistematica dei reati *lato sensu* patrimoniali. – 2. I nodi irrisolti dell'individuazione del *tempus* e del *locus commissi delicti* e della giurisdizione rispetto ai reati commessi nel *web*. – 3. *Cybersecurity* e diritto all'anonimato. – 4. La responsabilità da reato delle persone giuridiche: spunti per una miglior cooperazione pubblico-privato. – 5. Proposte per un miglior coordinamento delle norme incriminatrici *lato sensu* patrimoniali. – 6. Riflessioni conclusive tra necessità di prevenzione, cooperazione internazionale e migliore qualità del sistema normativo per una più efficace tutela (non solo penale) del patrimonio.

1. Considerazioni politico-criminali sul ricorso allo strumento penale per tutelare il patrimonio e sulla collocazione sistematica dei reati *lato sensu* patrimoniali

Nonostante gli attacchi informatici contro il patrimonio siano un fenomeno in rapida e continua crescita, il numero di condanne effettive per frodi informatiche, *cyberextortion*, ecc. è piuttosto basso, come dimostrano sia le statistiche, sia, soprattutto, lo scarso numero di pronunce giurisprudenziali in merito. Sulla base di questi dati, dunque, ci deve chiedere se lo strumento penale sia effettivamente il più idoneo a reprimere queste manifestazioni criminose, soprattutto in considerazione del fatto che le banche sono civilmente responsabili in caso di operazioni non autorizzate dal cliente effettuate a mezzo di strumenti elettronici. Infatti, gli artt. 73 e 74 della direttiva 2015/2366/UE relativa ai servizi di pagamento nel mercato interno, la c.d. direttiva PSD2 (v. *supra*, cap. I, par. 6), stabiliscono il principio per cui nel caso venga eseguita un'operazione di pagamento non autorizzata il prestatore di servizi di pagamento del pagatore è tenuto a rimborsarla a quest'ultimo, tranne nel caso in cui quest'ultimo abbia agito dolosamente o non abbia adempiuto agli obblighi previsti dalla direttiva con dolo o negligenza grave. Spetta dunque, all'istituto di credito fornire la prova della riconducibilità dell'operazione al cliente, nonché della sussistenza del dolo o della colpa grave di quest'ultimo[1].

Pertanto, si potrebbe ritenere che, trattandosi di fatti di criminalità lieve in campo patrimoniale, dato che i singoli prelievi non autorizzati sono limitati a qualche centinaio o massimo migliaio di euro, la previsione del risarcimento a favore del correntista sia più che

[1] V. da ultimo Cass. civ., sez. I, sentenza 20 maggio 2022, n. 16417. In senso conforme anche Cass. civ., sez. I, sentenza 3 febbraio 2017, n. 2950.

sufficiente e le sanzioni penali del tutto inutili. Tale assunto, tuttavia, non appare corretto per più ordini di motivi. Il primo è che il meccanismo del risarcimento del danno da parte dell'istituto di credito è previsto unicamente in caso di commissione di frodi informatiche e indebito utilizzo di strumenti di pagamento diversi dai contanti. Ma, come si è avuto modo di esaminare nel presente lavoro, i reati cibernetici contro il patrimonio sono in realtà un insieme più ampio, che comprende anche truffe, estorsioni, danneggiamenti, ecc. Per tutti questi casi non è previsto alcun meccanismo di ristoro. Per cui, ad esempio, in caso di compromissione irreversibile delle funzioni di un *device* causato dal *ransomware* è il proprietario dello stesso che si trova da solo a sopportare integralmente le spese per la riparazione o l'acquisto di un nuovo sistema informatico, oltre, eventualmente a subire la perdita data dall'eventuale pagamento del riscatto. Inoltre, il sistema di rimborsi previsto in caso di operazioni di pagamento non autorizzate non è certo gratuito e comporta un certo aggravio di costi per le banche, che poi finiscono per essere addossati ai correntisti tramite aumenti dei costi del canone o similari. Dunque, il fatto che sia prevista una forma di rimborso in caso di operazioni di pagamento non autorizzate è da accogliere senz'altro con favore, ma non è certo sufficiente a sostenere l'inutilità della sanzione penale per coloro che con le loro condotte illecite hanno cagionato un danno patrimoniale.

Inoltre, considerare unicamente il prelievo finale ai danni del singolo correntista e ritenere, quindi, che la distrazione di piccole somme di denaro non sia meritevole di sanzione penale significa non avere ben chiara la reale portata del fenomeno. Infatti, come esaminato (v. *supra*, cap. I, par. 4.1.), dietro la singola transazione non autorizzata vi è un vero e proprio sistema illegale di acquisto, scambio e cessione di credenziali, numeri di carte di credito, ecc., in cui operano associazioni a delinquere. Peraltro, il criminale informatico nella maggior parte dei casi effettua molti prelievi di piccole somme, spesso sotto la soglia di *alert* del correntista, proprio allo scopo di non essere individuato. Non appare, quindi, giustificabile ritenere che tali fatti non vadano sanzionati penalmente.

Va ribadito che il patrimonio è pur sempre un bene giuridico che è di sicuro rilievo costituzionale, perché funzionale allo sviluppo della personalità, riconosciuto anche a livello sovranazionale, che necessita di protezione anche penale dalle forme di aggressione maggiormente offensive. Gli attacchi informatici diretti contro il patrimonio non ledono mai solo quest'ultimo, ma anche altri beni giuridici di primaria importanza, quali la riservatezza informatica, l'integrità di dati e sistemi, l'identità digitale, ecc. Infatti, una volta subito un attacco, la vittima dovrà necessariamente cambiare *password*, credenziali e simili per non subire altri attacchi, ma, come si è esaminato, non sempre è possibile farlo, come avviene

nei casi in cui strumenti di identificazione siano ad esempio l'impronta digitale o il codice fiscale. Non si tratta, quindi, soltanto di questione relativa a "pochi spiccioli". Dunque, anche in ragione della plurioffensività degli attacchi informatici descritti nel presente lavoro, non si comprende il motivo per cui in quest'ambito la tutela penale dovrebbe essere fortemente ridimensionata o addirittura azzerata.

Il problema principale è dato dalla difficoltà di reprimere e perseguire fatti criminosi offensivi del patrimonio commessi sul *web*, luogo virtuale ove le indagini sono particolarmente difficoltose e farraginose, data la possibilità dei criminali informatici di agire sotto anonimato, nonché da remoto da qualsiasi parte del mondo, per cui spesso si rende necessaria l'attivazione di strumenti di cooperazione internazionale. Questo complica notevolmente le cose, anche perché ad oggi non esiste un'organizzazione sovranazionale deputata al controllo di *Internet* che possa intervenire per reprimere gli abusi. Si concorda, però, con quegli autori che contestano l'idea che il web possa essere una "zona franca" libera dal diritto solo perché quest'ultimo non possiede confini geografici definiti[2]. Infatti, ciò che non è lecito nel mondo reale non può certo diventare lecito nell'universo virtuale solo per via delle difficoltà specifiche che questo spazio a-territoriale pone. Si dovrà, semmai, fare uno sforzo ulteriore per garantire la legalità anche in tale spazio virtuale.

Il diritto penale non può quindi abdicare il suo ruolo chiave nella lotta globale al *cybercrime*: esso deve fungere da strumento di tutela per coloro i quali hanno subìto lesioni nel *web* ai loro beni giuridici protetti, prevedendo sanzioni afflittive e persuasive per coloro che non rispettano i diritti altrui, permettendo all' Autorità la repressione del fenomeno[3] . Per svolgere questo arduo compito è tuttavia necessario che la legge penale sia adeguata a perseguire la criminalità informatica. Essa quindi dev'essere in grado di rispondere continuamente all'evoluzione di *Internet* e delle nuove tecnologie, in considerazione della velocità del loro sviluppo tecnologico, utilizzando formule flessibili, ma senza violare il principio di determinatezza.

---

[2] PICOTTI L., Cybercrime *e diritto penale*, in *Diritto penale dell'informatica. Reati della rete e sulla rete*, cit., p. 709 ss., p. 720.

[3] «*Anche nel Cyberspace servono regole giuridiche riconoscibili e condivise, dotate di efficacia e suscettibili di applicazione coattiva, in ipotesi di mancata adesione o rispetto da parte dei destinatari, con ricorso, dunque, anche a mezzi sanzionatori formali e coercitivi, riservati ad autorità e giudici imparziali, in conformità ai principi dello Stato di diritto*» così PICOTTI L., *Quale diritto penale nella dimensione globale del cyberspace?*, in Wenin R., Fornasari G. (a cura di), *Diritto penale e modernità: le nuove sfide fra terrorismo, sviluppo tecnologico e garanzie fondamentali*, Atti del convegno Trento, 2 e 3 ottobre 2015, Napoli, 2017, p. 309 ss., p. 313.

Qualche considerazione merita l'aspetto della collocazione dei reati cibernetici contro il patrimonio. Come si è esaminato, infatti, essi non sono riuniti in un capo autonomo, ma collocati in diversi titoli accanto a fattispecie ritenute affini. Si ritiene che tale scelta, peraltro effettuata anche dai legislatori tedesco e spagnolo, nonostante alcuni svantaggi già segnalati nei capitoli precedenti, sia comunque la più appropriata. Infatti, appare anacronistica l'idea della creazione di un unico titolo del Codice penale ove inserire tutti i reati che possono essere commessi nel *web*. Se al momento dell'introduzione delle prime normative degli anni Novanta l'idea di raggruppare in un unico titolo i reati informatici poteva anche risultare efficace, oggi non è più così. Come si può notare dall'analisi effettuata nei capitoli precedenti, i reati cibernetici non possono essere circoscritti ad un numero chiuso o limitato di fattispecie[4]. È certamente vero che gli stessi presentano modalità esecutive concretamente nuove, caratterizzandosi per essere perpetrati attraverso il *web* o comunque mediante procedimenti di elaborazione dati, ma non per questo necessitano di essere tutti tipizzati in fattispecie *ad hoc*. La creazione di un nuovo titolo del Codice penale, ove raggruppare tutti i reati cibernetici, sarebbe assolutamente inutile, dato che l'elenco di fattispecie tradizionali che possono essere commesse attraverso la rete si allunga in continuazione, per cui richiederebbe un assiduo e regolare aggiornamento, che sarebbe però pur sempre tardivo. Dunque, si ritiene senz'altro più efficace la suddivisione attuale, in cui i reati informatici sono collocati accanto a fattispecie tradizionali ritenute affini per i beni giuridici tutelati.

È vero però che il raggruppamento dei reati informatici e cibernetici sopra esaminati in un unico titolo potrebbe evitare gli inconvenienti verificatisi in occasione della trasposizione delle direttive 2019/713/UE e 2013/40/UE, cui il nostro legislatore ha dato attuazione con due provvedimenti adottati a distanza di tempo ravvicinata, modificando unicamente le fattispecie presenti in un singolo titolo di reato, senza considerare il complesso sistematico delle norme collocate in altri titoli ed accentuando in questo modo il problema della sovrapposizione delle fattispecie incriminatrici in materia. Tuttavia, non è detto che il problema possa risolversi con un semplice raggruppamento delle fattispecie. Tale iniziativa, infatti, se non accompagnata da una generale rivisitazione delle fattispecie vigenti, con conseguente abrogazione o trasfusione in singole norme di quelle che oggi costituiscono veri e propri doppioni, rischia di rivelarsi non solo inutile, ma addirittura deleteria, poiché non solo non risolverebbe il problema dell'individuazione dei rapporti tra le fattispecie, ma

[4] PICOTTI L., *Diritto penale e tecnologie informatiche: una visione d'insieme*, cit., p. 51.

legherebbe indissolubilmente fattispecie a tutela del bene giuridico della riservatezza informatica alle lesioni patrimoniali, senza considerare che le condotte sanzionate in queste ultime fattispecie hanno una portata più ampia.

Va però evidenziato che in molti casi la giurisprudenza e la dottrina ritengono che i reati tradizionali presentino un disvalore maggiore qualora commessi in rete. Sul punto, già si è sottolineato che la giurisprudenza ha finito per ritenere applicabile alla quasi totalità dei casi di truffe perpetrate sui siti di *e-commerce* la circostanza aggravante della minorata difesa (v. *infra*, cap. III, par. 1). Ciò, però, non significa che sia necessaria la creazione di una fattispecie *ad hoc*, bensì, più semplicemente, che il trattamento sanzionatorio per questi casi vada adeguato. Per questo, il problema può benissimo essere risolto mediante l'introduzione di una circostanza aggravante speciale. In tal caso, però, è necessario verificare che non accada ciò che è successo con l'introduzione della circostanza aggravante della fattispecie di frode informatica del trasferimento di denaro, valore monetario o valuta virtuale di cui al co. 2, la quale, sovrapponendosi all'evento della fattispecie, trova per forza di cose applicazione nella quasi totalità dei casi. Tuttavia, l'introduzione di una specifica circostanza aggravante per il reato di truffa, qualora le trattative contrattuali si siano svolte integralmente a distanza e/o qualora il reo si sia avvalso della rete per raggirare la vittima, non appare comportare tale rischio.

Rispetto agli altri ordinamenti esaminati, la collocazione sistematica dei reati cibernetici che offendono il patrimonio nel nostro codice penale appare essere senz'altro la più funzionale, dato il loro raggruppamento in un unico titolo del codice penale, cosa che nello *Strafgesetzbuch* tedesco e nel *Código Penal* spagnolo non avviene. È poi vero che il Titolo XII contiene solo una parte dei reati analizzati nei capitoli precedenti e che vengono commessi in occasione di un attacco informatico contro il patrimonio, quali ad esempio l'accesso abusivo ex art. 615-*ter* c.p. e i reati contro la riservatezza informatica. Appare corretta, però, la decisione di collocare questi reati tra quelli contro l'inviolabilità del domicilio o contro l'inviolabilità dei segreti. Tali fattispecie, infatti, non vengono in rilievo unicamente negli attacchi informatici contro il patrimonio, ma hanno un ambito di applicazione molto più ampio, perché possono costituire il preludio di ulteriori reati più o meno gravi, dalla diffamazione alla rivelazione di segreti. La loro collocazione nel titolo riservato ai reati contro il patrimonio, dunque, rischierebbe di essere eccessivamente restrittiva, basti pensare al furto d'identità digitale. Quest'ultima manifestazione criminosa, infatti, è stata prevista soltanto come una circostanza aggravante del reato di frode informatica, senza però considerare che il fenomeno del furto d'identità ha una connotazione

ben più ampia, perché non si limita alle sole diminuzioni patrimoniali che da esso possono essere causate, ma può essere realizzato anche per ledere l'onore o la reputazione ed in generale il diritto all'identità personale altrui. Dunque, il raggruppamento di tutte le fattispecie configurabili in caso di attacco informatico contro il patrimonio in un unico titolo rischia di essere fuorviante. Caso a parte è unicamente quello dell'art. 615-*quinquies* c.p., che, effettivamente, è reato prodromico unicamente al danneggiamento informatico e che per questo motivo, come già osservato in passato[5], dovrebbe essere correttamente collocato nel "microsistema" normativo concernente i reati informatici.

Diverso discorso riguarda la falsificazione e l'indebito utilizzo di strumenti di pagamento diversi dai contanti. Neppure l'art. 493-*ter* c.p., infatti, è collocato nel titolo del Codice penale dedicato ai reati contro il patrimonio, bensì nel titolo dei delitti contro la fede pubblica dedicato alla falsità in atti. Tuttavia, l'indebito utilizzo di strumenti di pagamento diversi dai contanti è condotta assolutamente eterogenea rispetto alla falsificazione dello strumento stesso. In questo caso il bene giuridico tutelato in via prioritaria appare essere non tanto la funzionalità, stabilità e credibilità nel sistema dei pagamenti, dunque la pubblica fede, bensì proprio il patrimonio del titolare. In questo caso si ritiene che la soluzione adottata dal legislatore spagnolo, di scindere in due norme separate la falsificazione degli strumenti di pagamento diversi dai contanti rispetto all'utilizzo indebito degli stessi, collocando quest'ultima tra i reati contro il patrimonio, potrebbe apportare indubbi benefici. Infatti, come sopra evidenziato (v. *supra*, cap. III, par. 3), il fatto che l'utilizzazione di strumenti di pagamento diversi dai contanti sia inserita tra i reati a tutela della pubblica fede finisce per conferire alla norma in questione una connotazione pubblicistica. In questo modo, si esclude l'applicabilità alla fattispecie in questione della scriminante del consenso dell'avente diritto, con conseguenze paradossali. Infatti, se, ad esempio, un coniuge, impossibilitato a farlo, consegna una carta di credito all'altro affinché prelevi il contante disponibile e/o effettui determinati acquisti a proprio favore, sarà punibile penalmente con pena addirittura superiore rispetto a colui che si sia indebitamente introdotto nel sistema di *home banking* di uno sconosciuto ed abbia effettuato una serie di bonifici a suo favore. Tuttavia, nell'uso autorizzato di una carta di credito genuina da parte di colui che non ne è titolare non appare ravvisarsi alcuna lesione dell'interesse pubblico fondamentale "a che il

[5] In tal senso PICA G., *Diritto penale delle tecnologie informatiche*, cit., p. 109; SALVADORI I., *I reati contro la riservatezza informatica*, cit., p. 701; PICOTTI L., *La ratifica della Convenzione Cybercrime*, cit., p. 708.

sistema elettronico di pagamento sia sempre utilizzato in modo corretto"[6]. Dunque, la collocazione della fattispecie in questione tra i reati contro il patrimonio in senso stretto servirebbe senz'altro a superare tale aporia.

Si evidenzia, poi, che, al contrario di quanto potrebbe sembrare, la distinzione tra frode informatica da un lato e falsificazione ed indebito utilizzo di strumenti diversi dai contanti dall'altro non è affatto facile da individuare, in particolare con riferimento ai nuovi strumenti immateriali, quali ad esempio le *App* di *home banking* per *smartphone*. Infatti, la falsificazione dei dati informatici degli strumenti di pagamento può rientrare nella più ampia condotta di manipolazione o alterazione degli stessi, mentre l'indebito utilizzo in quella di '"intervento senza diritto", entrambe sanzionate dalla fattispecie di frode informatica. Neppure il legislatore europeo è riuscito ad individuare una chiara linea di demarcazione tra i tre diversi fenomeni tant'è che, come si è esaminato nel corso del presente lavoro, ciascuno dei tre legislatori europei esaminati ha adottato differenti soluzioni. Sul punto, tuttavia, si può evidenziare che in realtà la frode informatica e l'indebito utilizzo degli strumenti di pagamento tutelano il patrimonio del titolare del denaro, mentre la sanzione della condotta di falsificazione serve a garantire l'affidabilità e sicurezza degli strumenti di pagamento. Dunque, una soluzione per evitare duplicazioni sanzionatorie potrebbe essere quella di riformulare la fattispecie di frode informatica, in modo da comprendere espressamente al suo interno anche l'indebito utilizzo degli strumenti di pagamento diversi dai contanti, da collocare nell'ambito delle fattispecie a tutela del patrimonio. Per quanto riguarda la falsificazione in sé, invece, seppur finalizzata ad un illecito arricchimento, costituisce fenomeno distinto, meritevole di sanzione penale indipendentemente dal raggiungimento del profitto. Una soluzione soddisfacente, dunque, potrebbe essere di sanzionare a parte la falsificazione degli strumenti di pagamento diversi dai contanti rispetto all'indebito utilizzo, collocando la norma in questione, quella sì, nell'ambito dei reati a tutela della pubblica fede. Per evitare duplicazioni sanzionatorie si potrebbe, come ha fatto il legislatore tedesco, equiparare la pena prevista per la frode informatica a quella per la falsificazione degli strumenti di pagamento diversi dai contanti. Inoltre, per marcare nettamente la distinzione dalla frode informatica ed evitare duplicazioni sanzionatorie, si potrebbero prevedere due distinte disposizioni: la prima, che sanzionerebbe unicamente la falsificazione, potrebbe

[6] Cass. pen., sez. II, sentenza 18 settembre 2020, n. 27432; Cass. pen., sez. II, sentenza 18 aprile 2019, n. 34466; Cass. pen., sez. II, sentenza 15 novembre 2012, n. 45902; Cass. pen., sez. IV, sentenza 13 dicembre 2019, n. 2319; Cass. pen., sez. II, sentenza 18 luglio 2017, n. 40875; Cass. pen., sez. VII, ordinanza 12 dicembre 2016, n. 2835.

prevedere una clausola di sussidiarietà espressa a favore della frode informatica, mentre la seconda sanzionerebbe le ulteriori condotte previste nella direttiva 2019/713/UE, ovvero il possesso, la cessione e l'acquisizione di tali strumenti, condotte che non si pongono in rapporto di interferenza con la frode informatica.

Se la collocazione dei reati cibernetici che offendono il patrimonio appare condivisibile, da rivedere, invece, è la suddivisione interna dei reati contro il patrimonio tra quelli commessi "mediante violenza" e "mediante frode". Infatti, come si è esaminato nel presente lavoro, le nuove modalità di aggressione al patrimonio, messe a punto dai criminali informatici, rendono difficile operare una netta distinzione tra violenza e frode. Nelle frodi informatiche, infatti, non è la vittima che effettua la disposizione patrimoniale, bensì lo stesso reo che, tramite la manipolazione del sistema, riesce ad effettuarla all'insaputa del titolare del patrimonio. Nonostante ciò, in questi casi vi è spesso un seppur minimo apporto causale della vittima, la quale scarica il *malware* sul computer, fornisce per errore le sue credenziali, ecc. In questo caso, dunque, la rigida bipartizione tra reati a cooperazione artificiosa della vittima e reati ad usurpazione unilaterale si rivela inadeguata rispetto all'attuale fenomenologia, dato che gli attacchi informatici sono di forma "ibrida". Ciò vale anche per l'estorsione, che, come sopra esaminato, da sempre si fatica a ricondurre nell'una o nell'altra categoria (v. *supra*, cap. III, par. 1). Un discorso ulteriore può essere fatto per le fattispecie di riciclaggio: effettivamente in questo caso le modalità della condotta non contemplano l'utilizzo di violenza, ma neppure appare esservi una qualche forma di frode.

Si ritiene che sia corretto imperniare il sistema di classificazione dei reati contro il patrimonio sulla condotta, visto che il riferimento all'oggetto di tutela, adottato in Germania, ha mostrato limiti ancora maggiori. Tuttavia, si ritiene che per una maggior chiarezza sistematica sarebbe più opportuno operare ulteriori suddivisioni e distinguere le norme in microgruppi, quali, ad esempio "delle frodi", "delle sottrazioni", "dei danneggiamenti", "dell'occultamento di capitali illeciti", ecc. In questo modo si manterrebbe comunque il focus sulla condotta, ma si eviterebbe il raggruppamento di fattispecie molto diverse tra loro.

2. I nodi irrisolti dell'individuazione del *tempus* e del *locus commissi delicti* e della giurisdizione rispetto ai reati commessi nel *web*.

Le frontiere nazionali costituiscono un evidente ostacolo all'individuazione, alle indagini e alla persecuzione penale degli autori dei reati cibernetici. Questo perché il *cyberspace* ha messo in crisi i tradizionali principi di individuazione del *tempus* e del *locus commissi delicti*. Infatti, nel mondo reale il reato si consuma in un luogo più o meno

determinato del territorio, per cui si parte proprio dal territorio per assegnare la giurisdizione nazionale o la competenza tra giudici interni allo Stato. Nello spazio virtuale, invece, il territorio non ha rilevanza, ciò che conta sono i terminali, le connessioni, le reti e i dati, presenti e circolanti in ogni parte del mondo[7]. Va evidenziato che la struttura del *web* fu appositamente costruita per funzionare senza un previo controllo o una gestione centralizzata, essendo formata da connessioni, nodi e sistemi privi di un unico centro di scambio e controllo: per cui i circuiti attraverso i quali i dati e le informazioni circolano sono "orizzontali", imprevedibili per la loro automaticità e universali per la disposizione ed espansione della rete[8]. La dimensione a-territoriale della rete si è ulteriormente accentuata con la diffusione di dispositivi quali *smartphone*, *tablet*, computer portatili, ecc., che possono essere utilizzati per accedere al *web* in qualsiasi parte del globo, indipendentemente dal luogo di acquisto o di residenza del loro utilizzatore, nonché dei sistemi di *cloud storage*, ovvero sistemi utilizzati per l'archiviazione di dati, fotografie e documenti che utilizzano la rete Internet e cui si può accedere da qualsiasi parte del mondo con qualsiasi dispositivo.

Le peculiarità del *web* hanno dunque messo in crisi i tradizionali criteri per individuare la collocazione nel tempo e nello spazio delle condotte umane suscettibili di costituire reato. Le tradizionali nozioni di *tempus* e *locus commissi delicti* mal si adattano alla realtà virtuale, la quale, come si è visto, è dematerializzata e priva di qualcosa di anche vagamente simile ai confini nazionali[9].

Per quanto riguarda il *tempus commissi delicti*, va tenuto presente che il *web* consente la detemporalizzazione delle attività. Oggi le operazioni da svolgere possono essere programmate e svolte in automatico dal sistema. Non solo: se un tempo il passaggio fisico del denaro individuava il tempo di consumazione del reato contro il patrimonio, e quindi anche il luogo di commissione dello stesso, oggi non è più così. Infatti, come si è esaminato, non sempre il momento della disposizione di pagamento coincide con quello dell'effettivo accredito della somma di denaro, per non parlare della possibilità di annullare la disposizione e bloccarne il pagamento. Tutto ciò, come si è esaminato, ha notevoli influenze in merito al profilo temporale dei reati in questione.

Se, però, il problema dell'individuazione del *tempus commissi delicti* può essere risolto facendo ricorso ai tradizionali criteri, quindi facendo coincidere l'evento lesivo con l'effettivo accredito, diverso discorso va fatto per il *locus*.

[7] FLORES PRADA I., *Criminalidad informática*, cit., p. 313.
[8] *Ibid*., p. 314.
[9] FLOR R., *I limiti del principio di territorialità nel cyberspace*, cit., p. 1293.

Nei fatti che si svolgono nel mondo reale, infatti, è agevole individuare dove si è svolta l'azione o l'omissione, ovvero dove si è verificato l'evento. Al contrario, nell'universo virtuale questo è molto arduo, se non impossibile. Non a caso, sul punto si sono registrati diversi contrasti giurisprudenziali. Basti pensare alle difficoltà nell'individuazione del *locus commissi delicti* del reato di accesso abusivo a un sistema informatico o telematico, problematica sulla quale sono intervenute le Sezioni Unite (v. *supra*, cap. II, par. 2); ovvero di quello delle truffe commesse *online* (v. *supra*, cap. III, par. 1). Il problema, peraltro, non riguarda unicamente la fase della depauperazione patrimoniale della vittima, ma anche il successivo fenomeno del *cyberlaundering*. Se, infatti, il *tumbler* effettua molteplici scambi in criptovalute provento di reato, magari riscatto a seguito di *ransomware*, "confondendo" la catena blockchain per occultarne l'origine (v. *supra*, cap. I, par. 3.5), dove e quando può dirsi consumato il reato di riciclaggio? In assenza di un "tribunale internazionale del *web*" è, dunque, indispensabile trovare soluzioni alternative.

Se il principio di territorialità esige la determinazione del luogo di commissione del fatto, lo stesso ammette eccezioni in determinati casi. La legislazione penale nazionale può estendersi in relazione a condotte realizzate in altri Stati, le cui conseguenze si producono all'interno dei confini nazionali[10]. Il nostro legislatore prevede che il criterio basilare, in materia di efficacia della legge penale nello spazio, sia il principio di territorialità, anche se contemperato dal ricorso ai criteri di personalità, difesa e universalità[11]. Va però evidenziato che un conto è l'individuazione del *locus commissi delicti*, un altro quella dell'individuazione del giudice competente. Le due questioni sono strettamente correlate, perché in linea di principio il giudice competente è quello del luogo in cui il reato è stato commesso. Il codice di procedura penale, infatti, prevede all'art. 8 c.p.p. quale criterio principale quello della territorialità, per cui la competenza per territorio è determinata dal luogo in cui il reato è stato consumato. L'art. 9 c.p.p prevede però altri criteri suppletivi per il caso in cui la competenza territoriale non possa essere determinata ai sensi della norma precedente. Il co. 2 in particolare fa riferimento al criterio della personalità attiva, per cui giudice competente è quello ove risiede, dimora o è domiciliato l'imputato. Ulteriore criterio suppletivo è quello del luogo in cui ha sede l'ufficio del pubblico ministero che ha provveduto per primo a iscrivere la notizia di reato. In quest'ultimo caso, va evidenziato che la decisione quadro 2009/948/GAI sulla prevenzione e la risoluzione dei conflitti relativi

[10] FLORES PRADA I., *Criminalidad informática*, cit., p. 314.
[11] Per tutti FIANDACA G., LEINERI G., Sub *art. 6 c.p.*, in *Commentario breve al codice penale*, cit., p. 36 ss., p. 36 s.

all'esercizio della giurisdizione dei procedimenti penali, cui è stata data attuazione col d.lgs. n. 29/2016, prevede diversi strumenti in grado di evitare l'insorgere di procedimenti penali paralleli in relazione allo stesso fatto. In materia di responsabilità da reato degli enti, invece, si fa riferimento alla sede della persona giuridica destinataria del vantaggio. In prospettiva comparata, la Spagna è uno dei Paesi dove in materia di giurisdizione vige il c.d. principio di universalità, per cui già considera i giudici nazionali come "giudici universali", estendendo la sua competenza a reati commessi in qualsiasi parte del mondo indipendentemente dalla nazionalità dell'autore. L'art. 23.4 della *Ley Orgánica del Poder Judicial* n. 6 del 1° luglio 1985, infatti, consente ai giudici spagnoli di perseguire reati commessi in qualsiasi parte del mondo da cittadini spagnoli e da stranieri. Tale principio, però, non vale per tutti i reati, ma solo per quelli più gravi specificamente indicati dalla norma, per cui non è applicabile alla maggioranza dei reati informatici e cibernetici, se non per il caso di sabotaggio informatico correlato ad un reato terroristico (art. 23.4 lett. b) LOPJ)[12]. Il § 9 dello *Strafgesetzbuch* tedesco, invece, stabilisce quale criterio prevalente quello della personalità attiva.

La questione dell'individuazione del giudice competente viene affrontata anche dalla Convenzione *Cybercrime*. L'art. 22, intitolato "competenza", prevede l'obbligo per gli Stati aderenti di stabilire, nei casi elencati dalla norma, la propria competenza territoriale in relazione alle condotte descritte in tale strumento. È evidente, però, la sua obsolescenza sul punto, dato che prevede, quale criterio principale per stabilire la competenza territoriale, proprio il principio di territorialità, e solo in subordine fa riferimento al criterio della nazionalità del soggetto attivo[13]. Infatti, quando esso è stato redatto il *web* ancora non era diffuso come adesso e i *cloud* non erano ancora stati sviluppati, per cui ancora si poteva fare riferimento al luogo in cui il computer era fisicamente installato.

Per quanto riguarda i provvedimenti adottati dall'Unione europea, esaminati nei capitoli precedenti, in materia di giurisdizione sui reati cibernetici vengono previsti alternativamente i criteri della territorialità e della personalità attiva[14]. Ultimamente, però, è stato accolto anche il principio della personalità passiva. La direttiva 2019/713/UE relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti, infatti,

[12] FLORES PRADA I., *Criminalidad informática*, cit., p. 317.
[13] «Ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie per stabilire la propria competenza […], quando i reati siano commessi: a. nel proprio territorio; […] d. da un proprio cittadino, se l'infrazione è penalmente punibile là dove è stata commessa o se l'infrazione non rientra nella competenza territoriale di alcuno Stato».
[14] FLOR R., *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*, in A. Cadoppi, S. Canestrari, A. Manna e M. Papa (a cura di) *Cybercrime*, Torino, 2019, p. 141 ss., p. 191.

prevede la possibilità per lo Stato membro di stabilire la giurisdizione per uno dei reati di cui alla direttiva qualora lo stesso sia stato commesso contro uno dei suoi cittadini o contro una persona che risiede abitualmente nel suo territorio. In ogni caso, nessuno dei provvedimenti sovranazionali in materia prende espressamente posizione in ordine ai problemi generali in tema di giurisdizione e di competenza per i reati commessi nel *web*[15]. Il legislatore italiano, dunque, non è mai intervenuto in tal senso, lasciando inalterate sia le norme relative al *locus commissi delicti*, sia in materia di giurisdizione. Lo *status quo*, però, non appare per nulla soddisfacente. Infatti, in tutti quei numerosi casi in cui l'azione si svolge integralmente *online*, nell'impossibilità di individuare un luogo fisico di consumazione del reato si deve necessariamente fare riferimento ai criteri residuali di cui all'art. 9 c.p.p. per la determinazione del giudice competente. In questi casi, dunque, l'ipotesi residuale diviene quella ordinaria.

Neppure i criteri residuali appaiono soddisfacenti. Come sopra evidenziato, infatti, il co. 2 dell'art. 9 c.p.p. fa riferimento unicamente al domicilio, alla residenza o alla dimora del reo. Tuttavia, sono numerosi i casi di frodi informatiche, attacchi informatici, ecc. commessi da persone residenti all'estero, magari addirittura in Paesi che non hanno ratificato la Convenzione *Cybercrime* quali ad esempio la Russia, ai danni di cittadini italiani. In questi casi, però, il giudice italiano non è competente con riferimento al reato in questione e ciò comporta un importante *vulnus* di tutela per le vittime.

A tal proposito, va evidenziato che sia la direttiva 2019/713/UE, all'art. 12, che la direttiva 2013/40/UE, sempre all'art. 12, obbligano gli Stati membri ad adottare «*le misure necessarie a stabilire la propria giurisdizione per i reati di cui agli articoli da 3 a 8*». La procedura d'infrazione aperta nei confronti dell'Italia per il mancato recepimento della direttiva 2013/40/UE riguardava proprio quest'ultimo profilo: la mancata attuazione delle disposizioni relative alla giurisdizione[16]. Dunque, non avendo previsto nulla sul punto in sede di attuazione, il legislatore italiano non ha recepito correttamente la direttiva europea ed è assai probabile che in futuro vi saranno ulteriori contestazioni, se non addirittura l'apertura di ulteriori procedure di infrazione. È, dunque, opportuno che il legislatore italiano provveda quanto prima alla modifica delle norme in tema di giurisdizione per i reati informatici e/o di individuazione del *locus commissi delicti*.

[15] SEMINARA S., Locus commissi delicti, *giurisdizione e competenza nel cyberspazio*, 2012, p. 7, disponibile al sito https://www.flamminiiminuto-chiocci.it/public/pubblicazioni/Giurisdizione_italiana_per_diffamazione_internet_dall_estero.pdf.
[16] Dossier n. 294/2, cit., p. 84.

Una soluzione soddisfacente potrebbe essere quella di prevedere espressamente la giurisdizione italiana qualora la vittima risieda in territorio italiano[17], il che gioverebbe senz'altro alla speditezza dei procedimenti. Tuttavia, tale facoltà è stata riconosciuta dalla sola direttiva 2019/713/UE, previa comunicazione alla Commissione europea. È però vero che la lett. b) dell'art. 12 della direttiva 2013/40/UE prevede che lo Stato membro è tenuto ad assicurare la propria competenza giurisdizionale nel caso in cui il reato sia stato commesso contro un sistema di informazione presente nel suo territorio, indipendentemente dal fatto che l'autore del reato fosse o meno fisicamente presente nel suo territorio al momento della commissione del reato. Dunque, nulla vieta di fare riferimento alla collocazione del sistema informatico oggetto dell'attacco in questione, ed indirettamente, così, al luogo in cui risiede la vittima. Si deve allora auspicare un nuovo intervento normativo volto a correggere tale inottemperanza.

Per il *cyberlaundering* il discorso è più complesso, così come per tutti quei reati informatici in cui la vittima del reato non sia identificabile in una determinata persona fisica o giuridica, dato che riguardano sistemi informatici "di pubblica utilità". Nel riciclaggio digitale integrale, poi, dato che il denaro è *ab origine* dematerializzato, è impossibile individuare un luogo fisico cui fare riferimento per l'individuazione del Tribunale competente. In questo caso, dunque, il criterio del luogo di residenza, dimora o domicilio del reo appare l'unico che abbia un qualche significato. Diverso discorso, invece, va fatto per la condotta di impiego del denaro provento di *cyberlaundering*, dato che qui è possibile individuare un luogo fisico di collegamento. Per quanto riguarda, infine, i danneggiamenti informatici e i sabotaggi informatici che riguardano reti "di pubblica utilità", va evidenziato che gli stessi sono reati di evento, per cui si può individuare, quale criterio di collegamento per stabilire la competenza territoriale, il *locus* nel quale i dispositivi o i server danneggiati sono situati o comunque, nel caso si tratti di danneggiamento di dati contenuti in un *cloud*, il luogo dove si sono prodotti gli effetti del sabotaggio. In ogni caso, va evidenziato che per i sabotaggi informatici più gravi, che coinvolgono le infrastrutture dello Stato, vi è pur sempre il principio di ubiquità accolto dall'art. 7 c.p. per i reati lesivi di primari interessi dello Stato.

Si auspica, quindi, che il nostro legislatore, anche sulla base di quanto richiesto dalle direttive sopra menzionate, intervenga quanto prima al fine di prevedere nuovi criteri chiari per la determinare la giurisdizione e competenza territoriale per i reati cibernetici in

[17] Per la stessa soluzione in caso di vittima determinata anche CAMPLANI F., Locus commissi delicti, *norme di collegamento e reati informatici a soggetto passivo indeterminato*, in *Arch. pen*., 2020, n. 2, p. 1 ss., p. 6.

questione, in modo da garantire una maggiore tutela per le vittime ed evitare dispendiosi conflitti di giurisdizione, attribuzione o competenza.

3. *Cybersecurity* e diritto all'anonimato

Come evidenziato anche nei capitoli precedenti, i moderni criminali che si avvalgono della tecnologia informatica possono anche avvalersi del prezioso scudo dell'anonimato. A tal proposito, va ricordato che per chi dispone di specifiche conoscenze informatiche è operazione semplice oscurare il proprio indirizzo IP (*Internet Protocol*), ovvero l'etichetta che identifica ogni dispositivo collegato al *web*.

Tuttavia, normalmente, per navigare nel *web* o per usufruire di determinati servizi digitali non è necessario rivelare sempre ed in ogni caso la propria identità a chiunque, esattamente come avviene nel mondo reale. Molto dibattuta, quindi, è la questione se esista o meno è il diritto all'anonimato di chi comunica o utilizza la rete.

Al diritto all'identità personale si accompagna il dovere per il soggetto, in talune circostanze, di rivelare la propria identità. Come esaminato in precedenza (v. *supra*, cap. IV, par. 2), la normativa antiriciclaggio impone, all'art. 17 ss. d.lgs. 231/2007, l'identificazione del cliente di banche e/o intermediari finanziari, che avviene con l'acquisizione di copia di un documento d'identità in formato cartaceo o elettronico. In materia di firma elettronica, invece, l'art. 9 del Regolamento eIDAS (v. *supra*, cap. I, par. 9.2), prevede l'obbligo di identificazione dell'utilizzatore per il rilascio dei mezzi di identificazione elettronica.

In questo caso, come avviene per il diritto al nome, la prospettiva dell'ordinamento è duplice, perché oltre alla tutela del diritto dell'individuo al rispetto della propria immagine nella comunità vi è anche l'interesse della collettività a che ciascuno dei componenti della società possa essere distinto dagli altri[18]. In ambito penale, poi la sicurezza in merito all'identità del soggetto è fondamentale, dato che l'art. 27 Cost. sancisce che «*la responsabilità penale è personale*». Al divieto, quindi, di essere puniti per l'altrui fatto illecito si accompagna la necessità della certezza nell'identificazione del reo.

L'interesse pubblico a che i soggetti rivelino in talune circostanze la propria identità personale è in alcuni casi penalmente protetto. Alla "falsità personale" è, infatti, dedicato il capo IV del titolo VII del libro II del codice penale, che raccoglie le norme poste a tutela della pubblica fede, lesa con l'alterazione di elementi che identificano una persona o le sue

[18] BAVETTA G., voce *Identità (diritto alla)*, in *Enc. dir.*, vol. XIX, Milano, 1970, p. 953 ss., p. 954.

qualità che ne condizionano il ruolo nella società civile[19]. Per quanto riguarda specificamente la firma elettronica, l'art. 495-*bis* c.p., inserito dalla l. 18 marzo 2008, n. 48 della Convenzione *cybercrime*, sanziona penalmente chiunque dichiara o attesta falsamente al soggetto che presta servizi di certificazione delle firme elettroniche l'identità o lo stato o altre qualità della propria o dell'altrui persona[20]. Tuttavia, nel caso in cui non vengano pregiudicati interessi di altri soggetti e laddove manchi manca un'espressa previsione normativa che lo imponga, non sussiste un obbligo di rivelare la propria identità. Si può infatti agevolmente affermare che la simulazione dell'identità sia vietata solo qualora venga posta in essere per scopi illeciti[21].

In molti casi il cambiamento d'identità è considerato perfettamente legale[22]. Un esempio di lecita simulazione della propria identità personale lo si trova nell'art. 497, co. 2-*bis*, c.p.p., nella parte in cui sancisce che negli atti preliminari all'esame testimoniale «*gli ufficiali e gli agenti di polizia giudiziaria, anche appartenenti ad organismi di polizia esteri, i dipendenti dei servizi di informazione per la sicurezza, gli ausiliari, nonché le interposte persone, chiamati a deporre, in ogni stato e grado del procedimento, in ordine alle attività svolte sotto copertura ai sensi dell'articolo 9 della legge 16 marzo 2006, n. 146, e della legge 3 agosto 2007, n. 124, e successive modificazioni, invitati a fornire le proprie generalità, indicano quelle di copertura utilizzate nel corso delle attività medesime*».

Si può dunque ritenere che, almeno di regola, sia legittimo l'occultamento della propria identità, purché, come si è detto, non vi sia un obbligo di dichiarare le proprie generalità e non si perseguano finalità illecite: se il soggetto non ha l'obbligo di rivelare la propria identità può dunque mantenere l'anonimato e tacere sulla propria identità personale e le sue qualità[23].

Per quanto riguarda specificamente l'universo virtuale, vi è chi ha evidenziato che dato anonimo ed *Internet* costituiscono un binomio già dagli albori della diffusione di quest'ultimo mezzo[24]. Si è, infatti, sostenuto che l'anonimato sarebbe nel "codice genetico"

---

[19] Cfr. FIANDACA G., MUSCO E., *Dir. pen., PS*, cit., p. 617.
[20] Per approfondire v. PICOTTI L., *La ratifica della Convenzione Cybercrime*, cit., p. 701 ss.
[21] Così BAVETTA G., voce *Identità (diritto alla)*, op. cit., p. 954.
[22] In questo senso KOOPS B.J., LEENES R., *Identity Theft, Identity Fraud and/or Identity-related Crime*, in *DuD*, 2006, vol. 30, n. 9, p. 553 ss., p. 553, I quali evidenziano che: «*In all subtypes, the identity change can be perfectly lawful. For instance, a Tony Blair doppelgänger can walk the streets of London to see how the public reacts; a wife can lend her bank card to her husband to purchase something; the prince and the pauper can swap lives for a day; and Eric Arthur Blair may well choose a pseudonym to publish his books*».
[23] Cfr. BAVETTA G., voce *Identità (diritto alla)*, cit., p. 954.
[24] La nozione legislativa di dato anonimo è contenuta all'art. 4, co. 1, lett. n) del d.lgs. 196 del 2003 (cd. "codice privacy"): «*il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile*».

della rete, che dev'essere tutelato e preservato, dato che costituisce uno strumento necessario per limitare forme sempre più pervasive di sorveglianza da parte di poteri pubblici o privati[25].

È da ricordare che lo strumento informatico col quale si svolge la navigazione è identificabile con il suo indirizzo IP (*Internet Protocol*) o col suo *Domain Name* (espressione linguistica del primo), che però possono essere associati solo al *server* o comunque al dispositivo informatico, non all'utente che li utilizza. Di regola, quindi, colui che naviga in rete si trova ad operare in una situazione di anonimato, poiché ad essere visibile e conosciuto è solo l'indirizzo del sistema, non l'identità del suo utilizzatore che, nei sistemi accessibili al pubblico, quali ad esempio quelli presenti in un *Internet point*, può essere chiunque.

Secondo un settore della dottrina, l'anonimato in rete dovrebbe essere considerato addirittura come condizione giuridica "normale", mentre l'identificazione andrebbe qualificata come un'eccezione rispetto alla regola dell'anonimato [26].

A questo punto occorre operare una necessaria distinzione: per quanto riguarda la fruizione di determinati servizi sul *web*, quali ad esempio quelli firma elettronica o bancari, è comunque richiesta per legge una qualche forma di identificazione. In questo caso le dichiarazioni mendaci sulla propria identità sono punite penalmente dalle fattispecie contemplate nel capo del codice penale relativo alla falsità personale[27], tra cui l'art. 495-*bis* c.p. Dunque, l'anonimato non costituisce affatto una caratteristica intrinseca del mezzo: quando si utilizzano identità digitali "necessarie"[28] non si mantiene l'anonimato, non solo perché per ottenerle è necessaria una previa procedura di identificazione, ma anche perché per l'importanza delle stesse l'ordinamento richiede che vi sia coincidenza tra identità personale e digitale (anche se pure in questo caso vi è il rischio di sostituzioni di persona o false dichiarazioni alle autorità o al certificatore di firma elettronica).

Se non addirittura composte da nome e cognome di cui il soggetto è titolare nella vita reale, o dal codice fiscale, esse comunque contengono dati personali e sono costruite in modo tale da garantire il più possibile la coincidenza tra identità digitale e "reale" dell'utilizzatore.

Per quanto riguarda la firma elettronica qualificata o digitale, poi, l'esigenza di certezza dell'ordinamento è tale che il legislatore ha persino inserito una presunzione relativa per cercare di risolvere le difficoltà probatorie legate al fatto che l'indirizzo IP è riconducibile

---

[25] Cfr. VIGEVANI G.E., *Anonimato, responsabilità e trasparenza nel quadro costituzionale italiano*, in *Dir. inf. inf.*, n. 2, 2014, p. 207 ss., p. 207.
[26] FINOCCHIARO G., *Conclusioni*, in ID. (a cura di), *Diritto all'anonimato*, Padova, 2008, p. 411 ss., p. 414.
[27] Si pensi a titolo esemplificativo all'art. 495-*bis* c.p., che punisce: «*chiunque dichiara o attesta falsamente al soggetto che presta servizi di certificazione delle firme elettroniche l'identità o lo stato o altre qualità della propria o dell'altrui persona è punito con la reclusione fino ad un anno*».
[28] Sulla distinzione tra le diverse tipologie di identità digitali si richiama quanto già esposto al cap. I, par. 2.3.

solo alla macchina e quindi non permette automaticamente di risalire all'effettivo utilizzatore, ben potendo essere diverso dal proprietario[29]. Non solo: come si è appena evidenziato, la falsità al certificatore di firma elettronica è penalmente sanzionata dall'art. 495-*bis* c.p.

Il discorso che segue sull'anonimato non può essere quindi riconducibile alle identità digitali istituzionali e già, quindi, è evidente che vi sono ulteriori esigenze che prevalgono rispetto alla facoltà di rimanere anonimi mentre si naviga in rete.

Quanto viene ora esposto riguarda quindi le "altre" identità digitali, quelle che vengono create dal soggetto in luoghi virtuali nei quali non esiste alcun obbligo di utilizzo della propria identità reale. Infatti, una persona può, nello sviluppare la propria identità virtuale, scegliere un nome di fantasia (c.d. *nick*), e restare così nell'anonimato. Questo non ha necessariamente una connotazione negativa o illecita: esso impedisce massicci interventi invasivi sul diritto alla riservatezza da parte di imprese quali *Google* o *Facebook*, le quali sfruttano economicamente i dati riguardanti abitudini, gusti e comportamenti dei naviganti nel *web* (c.d. *profiling*) consentendo ad altre aziende di utilizzarli per una pubblicità mirata[30]. Si aggiunga che la facoltà di non essere identificati consente al dissidente politico, in fuga dal regime dittatoriale cui sottostà il suo Paese, di denunciare al mondo intero quanto ivi sta accadendo, senza il rischio di essere identificato[31].

Si è anche discusso se l'anonimato possa costituire un diritto fondamentale dell'individuo, dato il binomio indissolubile che lo lega ad *Internet*[32]. Per stabilire se possa trattarsi di un bene costituzionalmente protetto vanno individuati gli articoli della Costituzione che possono, almeno implicitamente, venire in rilievo in questo ambito. Anche in questo caso, però, come per il diritto all'identità personale, la carta fondamentale non contiene tra le sue norme alcun riferimento all'anonimato.

Un settore della dottrina[33] ha preso come punto di partenza il diritto alla riservatezza,

---

[29] L'art. 21 d.lgs. 82/2005 cit. sancisce che «*l'utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare, salvo che questi dia prova contraria*».

[30] Secondo l'opinione di autorevole dottrina infatti «*il valore generale dell'anonimato e dello pseudonimo in rete è confermato dalla constatazione che solo così è possibile sottrarsi ad interferenze nella propria vita che si traducano in aggressioni particolarmente gravi, in discriminazioni, molestie, limitazioni della libertà di espressione, esclusione da circuiti comunicativi»* in tal senso RODOTÀ S., *Il diritto di avere diritti*, Bari, 2012, p. 392.

[31] *Ibid*.

[32] Cfr. VIGEVANI G.E., *Anonimato, responsabilità e trasparenza nel quadro costituzionale italiano,* in *Dir. inf. inf.*, n. 2, 2014, p. 207 ss., p. 207. L'autore si chiede se il diritto all'anonimato nell *web* sia necessario per garantire a tutti la libertà di espressione senza il timore di ritorsioni, questo anche per il fatto che le tecnologie consentono «*un permanente controllo delle vite degli individui».*

[33] VIGEVANI G.E., *Anonimato*, cit., p. 210.

riconducibile agli artt. 2, 3, 13, 14 e 15 Cost., che consiste nel diritto di escludere gli altri dalla conoscenza dei propri dati personali e delle proprie generalità. Il diritto a non rivelare la propria identità ha trovato in seguito tutela espressa nell'art. 3 d.lgs. 196/2003 (c.d. "Codice *privacy*"), il quale sancisce che «*i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità*». Anche la dottrina tedesca evidenzia che il diritto all'anonimato non è tra quelli espressamente riconosciuti dalla Costituzione tedesca, né è stato ancora riconosciuto come autonomo diritto dalla Corte costituzionale. Tuttavia, si sostiene che l'anonimato in *Internet* sarebbe espressione di due diritti fondamentali riconosciuti, ovvero il diritto alla libertà di espressione (Art. 5 Abs. 1 Satz 1 GG) e il diritto fondamentale all'autodeterminazione informativa (Art. 1 Abs. 1 GG in combinato disposto con l'Art. 2 Abs. 1 GG)[34], già esaminati nel capitolo precedente (v. *supra*, cap. V, par. 1.1).

In alcuni casi il nostro legislatore ha riconosciuto un diritto all'anonimato. Si pensi, a titolo esemplificativo, al riconoscimento del diritto del tossicodipendente, che si sottoponga a una terapia riabilitativa volontaria, a che la sua scheda sanitaria non contenga le generalità né altri dati che possano aver funzione di identificarlo (art. 120 D.P.R. 9 ottobre 1990, n. 309); all'obbligo per il personale sanitario ed amministrativo di garantire l'anonimato dei dati relativi al donatore e al ricevente per le attività di prelievo e di trapianto di organi (art. 18, co. 2, l. 1 aprile 1999, n. 91); nonché il diritto della madre di scegliere l'anonimato al momento della nascita del figlio (l. 4 maggio 1983, n. 184).[35]

Tutto questo, però, non è sufficiente a riconoscere l'esistenza di un diritto di portata generale all'anonimato in *Internet*. Ed in tal senso si è affermato che in realtà il diritto all'anonimato non è che un diritto frammentario, che non ha portata generale, ma è relativo e strumentale all'esercizio di altri diritti di rilievo costituzionale, quali la riservatezza, l'identità personale, la salute e la vita[36]. Non è, pertanto, possibile affermare che nel nostro ordinamento vi sia un generale diritto all'anonimato, né che esso possa essere ricavato in via automatica dal diritto alla riservatezza.

Secondo alcuni studiosi la Costituzione ammette la facoltà di celare la propria

[34] WEBER M., *Die Strafbarkeit von Plattformbetreibern im Darknet*, cit., p. 43.
[35] VIGEVANI G.E., *Anonimato*, cit., p. 210.
[36] *Ibidem*.

identità per garantire la tutela dei propri diritti fondamentali, anche nel *web*[37]. In tale contesto l'anonimato assumerebbe la funzione di garantire il diritto alla ricostruzione della corretta identità di un soggetto, messa a repentaglio da molestie e schedature non autorizzate[38] e sarebbe strumentale rispetto all'effettivo esercizio del diritto alla riservatezza e del diritto alla protezione dei propri dati personali, concretandosi in una forma di controllo e nella possibilità di esclusione[39].

Va altresì tenuto in considerazione che, oltre alla garanzia dell'anonimato per la tutela dei propri dati personali, vi sono altri interessi ugualmente importanti che richiedono un contemperamento, primo tra tutti la sicurezza della rete e dei dispositivi informatici. Anche a voler considerare l'anonimato come un diritto, è necessario tener presente che nel nostro ordinamento non esistono diritti assoluti[40]. La rete consente di compiere moltissime attività, anche illecite[41] e ciò pone quindi il problema di tutelare le vittime del *cybercrime*, facendo in modo che i criminali, che celano la loro vera identità dietro lo scudo dell'anonimato, non perseverino impunemente nelle loro attività criminose.

Un limite al riconoscimento dell'anonimato *online* è previsto dall'art. 132 d.lgs. n. 196/2003 cit. per l'accertamento e la repressione dei reati[42]. Il fornitore telefonico che permette all'utente di accedere alla rete di fatto è tenuto per legge a registrare la sua vera

---

[37] Così VIGEVANI G.E., *Anonimato*, cit., p. 211, il quale sostiene che «*se non pare ricavabile dal testo costituzionale un autonomo diritto all'anonimato, si può, sia pure con qualche margine di approssimazione, ritenere che la Costituzione consenta e garantisca a una persona di celare le proprie generalità quando si tratti di tutelare i diritti della sfera individuale*». L'autore aderisce alla tesi di Finocchiaro, secondo la quale «*la differenza fra il trattamento dei dati personali oggi e venti anni fa è che oggi lasciamo sempre delle tracce e delle informazioni e non lasciarle è molto difficile. L'anonimato, quindi, dovrebbe essere considerato oggi non soltanto strumentale all'effettivo esercizio del diritto alla protezione dei dati personali e alla riservatezza, ma come una forma sia di controllo sui dati e sulle informazioni, che di esclusione di altri dalla conoscenza di tali dati e informazioni e viene a configurarsi quindi come modalità di esercizio della libertà positiva, che si concreta nel controllo, e nella libertà negativa, costituita dall'escludere gli altri*», così FINOCCHIARO G., *Conclusioni*, in ID. (a cura di), *Diritto all'anonimato*, cit., p. 414.

[38] Vigevani definisce il diritto all'anonimato come «*la pretesa dell'individuo a rendersi assente dall'arena dell'informazione*» in VIGEVANI G.E., *Anonimato*, cit., p. 211.

[39] FINOCCHIARO G., *Conclusioni*, in ID. (a cura di), *Diritto all'anonimato*, cit., p. 414.

[40] «*Con il diffondersi dei mezzi di controllo, sempre più presenti, l'anonimato assume il carattere di uno spazio di libertà, da garantire non soltanto strumentalmente, ma in sé. Tuttavia, trattandosi di una forma di esercizio del diritto alla protezione dei dati personali e alla riservatezza, come questi è destinato ad un continuo bilanciamento con altri diritti fondamentali. L'anonimato non può essere assoluto*», in tal senso FINOCCHIARO G., *Conclusioni*, in ID. (a cura di), *Diritto all'anonimato*, cit., p. 414.

[41] così CIPOLLA P., *Social network, furto di identità e reati contro il patrimonio*, in *Giur. mer.*, n. 12, 2012, p. 2672 ss., p. 2676.

[42] Nel primo comma l'articolo sancisce che: «*fermo restando quanto previsto dall'articolo 123, comma 2, i dati relativi al traffico telefonico sono conservati dal fornitore per ventiquattro mesi dalla data della comunicazione, per finalità di accertamento e repressione dei reati, mentre, per le medesime finalità, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, sono conservati dal fornitore per dodici mesi dalla data della comunicazione».*

identità[43]. Non si può scordare inoltre che è sempre possibile risalire all'indirizzo telematico dell'apparecchio (*device*) utilizzato per connettersi al *web*, ma non all'operatore sull'*hardware*, proprio per il fatto che l'indirizzo IP è associato alla macchina, non all'utilizzatore e più persone possono impiegare lo stesso *computer*.

Ad oggi anche se non esiste un vero e proprio diritto all'anonimato, non esistono neppure disposizioni che impongano una dichiarazione veritiera circa le proprie generalità utilizzate in rete[44]. Anche i provvedimenti adottati in materia di *cybersecurity*, infatti, si concentrano prevalentemente sulla necessità di portare a conoscenza il fatto dell'avvenuto attacco informatico. Una soluzione potrebbe essere quella del c.d. "anonimato risalibile"[45], con sistemi che certifichino la corrispondenza tra identità anagrafica e virtuale del soggetto, come accade già per quelle istituzionali ("necessarie") oppure per la firma digitale. Tale soluzione non è però agevolmente praticabile per tutte le tipologie di identità digitale, dal momento che un sistema di controllo capillare implicherebbe grosse difficoltà di attuazione, oltre a notevoli ritardi nell'attivazione dei servizi elettronici da parte del fornitore[46]. Oltretutto non è chiaro il motivo per cui si dovrebbe obbligare l'utente in ogni caso e per qualsiasi servizio *online* a rivelare la propria identità anagrafica, mentre nella vita reale questo non sarebbe quasi mai necessario: è opportuna quindi una soluzione che contemperi in maniera più efficace i diversi interessi.

Vi è chi fa presente che in realtà è irrazionale ogni atteggiamento di sospetto verso l'anonimato in rete, visto che forme analoghe di anonimato che si riscontrano in rete, ad esempio l'utilizzo di uno pseudonimo per *chattare* su un *social network*, si riscontrano anche nel mondo reale. Molti artisti utilizzano uno pseudonimo, senza dimenticare le comunicazioni con annunci rivolte ad un pubblico indifferenziato, che ad oggi ancora si trovano sui giornali. Si concorda con chi ritiene che appare iniquo e illogico, oltreché inutile, introdurre un divieto assoluto di comunicare anonimamente nel *web*[47]. Una soluzione potrebbe essere quella di obbligare i *providers* ad indentificare formalmente tutti i soggetti con cui stipulano il contratto di accesso alla rete, conservando in forma riservata le generalità dell'utente. In questo modo l'utente non è obbligato a svelare la sua identità al prossimo con

[43] PELLINO E., *L'anonimato su Internet,* in FINOCCHIARO G. (a cura di), *Diritto all'anonimato*, cit., p. 298.
[44] *«The point is simply that today's digital world lets us, in fact almost requires us, to choose a new digital identity almost daily. It's up to each one of us to develop a consistent pattern for that identity because there is no rule of law governing that process»* ARESTY J., *Digital Identity*, cit., p. 23
[45] Soluzione proposta da TRUCCO L., cit., p. 118
[46] Di quest'avviso ZICCARDI G., voce *"Furto d'identità"*, cit., p. 254.
[47] PICA G., *Diritto penale delle tecnologie informatiche*, cit., p. 278.

cui comunica, ma è comunque possibile risalire alla sua identità nel caso della commissione di illeciti a danno di terzi[48]. Anche questa soluzione, però, non appare facilmente praticabile.

L'unica soluzione allo stato attuabile è, quindi, individuare una serie di servizi fruibili dal *web* che per la loro importanza necessitano che la corrispondenza tra identità digitale utilizzata per l'accesso e identità personale dell'utilizzatore sia verificata ed esclusivamente in questo caso imporre procedure di validazione e/o controllo dell'identità. Anche questa, però, non è un'operazione facile, perché già l'individuazione dei "servizi fondamentali" per i quali richiedere un certo tipo di autenticazione non è banale e vi è il rischio che le scelte in merito siano fin troppo caute o, al contrario, restrittive. D'altra parte, però, non è neppure pensabile creare una barriera d'accesso al *web* imponendo a chiunque di fornire le proprie generalità, trattandosi di adempimento sproporzionato, che comporta notevoli costi e che non trova corrispondenza nel mondo reale.

4. La responsabilità da reato delle persone giuridiche: spunti per una cooperazione pubblico-privato

La frode informatica, seppur parzialmente, è ricompresa nel catalogo dei reati presupposto per la responsabilità da reato degli enti sin dall'introduzione del d.lgs. 8 giugno 2001, n. 231. L'art. 24 del decreto in questione, infatti, fa riferimento esclusivamente alla frode informatica commessa in danno dello Stato o di altro ente pubblico, non alla frode informatica *tout court*. I reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, invece, furono aggiunti dal d.lgs. n. 231/2007, mentre l'autoriciclaggio fu aggiunto dall' art. 3, co. 5, lett. a) l. 186/2014. Altri reati informatici furono poi inseriti nel catalogo di reati presupposto dalla l. n. 48/2008 di ratifica della convenzione *cybercrime*, per rispondere all'esigenza di difendere la collettività da reati "provenienti" dall'interno delle società[49]. In questo modo, infatti, il nostro legislatore ha dato attuazione all'art. 12 e 13 par. 2 della Convenzione *cybercrime*, nonché all'art. 9 della Decisione quadro 2005/222/GAI, oggi sostituita dalla direttiva 2013/40/UE, contenenti il vincolo per gli Stati aderenti ad adottare le misure necessarie per poter ritenere le persone giuridiche responsabili dei reati informatici commessi per loro conto da persone fisiche che agiscano sia individualmente che come membri di organi della persona giuridica[50]. In tale

[48] *Ibid*.
[49] FONDAROLI D., *La responsabilità di persone giuridiche ed enti per i reati informatici ex D.Lgs. n. 231/2001*, in *Cybercrime*, cit., p. 193 ss., p. 201.
[50] PICOTTI L., *La ratifica della Convenzione Cybercrime*, cit., p. 716.

ultima occasione, fu inserito nel d.lgs. 231/2001 l'art. 24-*bis*, col quale sono stati aggiunti al catalogo dei reati presupposto per la responsabilità da reato degli enti al co. 1 tutte e quattro le fattispecie appartenenti al "microsistema" dei danneggiamenti informatici, l'accesso abusivo ex art. 615-*ter* c.p., nonché i reati in materia di intercettazioni informatiche o telematiche di cui agli artt. 617-*quater* e 617-*quinquies* c.p. Al co. 2, invece, puniti con sanzione minore, sono stati aggiunti al catalogo i reati le fattispecie di cui agli artt. 615-*quater* e 615-*quinquies* c.p. Tuttavia, nonostante il nome della rubrica dell'art. in questione, ovvero «*Delitti informatici e trattamento illecito di dati*», tra i reati ivi elencati non figura nessuno dei reati previsti dal c.d. codice *privacy*, tantomeno il reato di trattamento illecito di dati personali di cui all'art. 167 codice *privacy*[51].

Da sempre la dottrina ha criticato la scelta del nostro legislatore di non inserire la frode informatica come tale nel catalogo dei reati presupposto di cui al d.lgs. 231/2001, esclusione da sempre ritenuta bizzarra, irragionevole e ingiustificata[52]. Il d.l. n. 93/2013, insieme all'introduzione del co. 3 all'art. 640-*ter* c.p., aveva provveduto anche ad inserire nell'art. 24-*bis* del d.lgs. n. 231/2001 il reato di frode informatica aggravato dalla sostituzione dell'identità digitale nel catalogo dei reati presupposto della responsabilità degli enti, oltre alla diversa fattispecie di indebito utilizzo, falsificazione, alterazione e ricettazione di carte di credito o di pagamento, nonché i delitti (ma non le contravvenzioni) in materia di violazione della *privacy* previsti dal d.lgs. n. 196/2003[53]. Tuttavia, in sede di conversione, è stato eliminato il comma che originariamente disponeva la responsabilità degli enti anche per questi reati. Le ragioni di tale scelta legislativa non sono chiare, ma secondo alcuni autori appare probabile che si sia preso atto che i soggetti interessati (quali istituti di credito e società di telecomunicazioni) non fossero attrezzati per adeguarsi a tale previsione, che avrebbe necessariamente richiesto maggiori controlli interni e più efficaci modelli organizzativi antifrode per sfuggire alle sanzioni *ex* d.lgs. n. 231/2001 cit., non attuabili in breve periodo [54].

Con il d.lgs. n. 184/2021, di attuazione della direttiva 2019/713/2019, il nostro legislatore è intervenuto nuovamente anche in materia di responsabilità da reato degli enti, introducendo il nuovo articolo 25-*octies*.1, che sanziona l'ente nel cui interesse o vantaggio

[51] SARZANA DI S. IPPOLITO C., *La legge di ratifica della Convenzione di Budapest*, cit., p. 1572 s.
[52] In tal senso BELTRANI S., *Reati informatici e d.lgs. 231/2001 alla luce della legge di attuazione della Convenzione di Budapest*, in *Resp. amm. società e degli enti*, 2008, n. 4, p. 21 ss., p. 24; PICOTTI L., *La ratifica della Convenzione Cybercrime*, cit., p. 716; p. SARZANA DI S. IPPOLITO C., *La legge di ratifica della Convenzione di Budapest*, cit., p. 1573.
[53] PISTORELLI L., *Relazione Ufficio del Massimario Cassazione*, n. III/01/2013, cit.
[54] CAJANI F., *La tutela penale dell'identità digitale*, cit., p. 1099.

siano stati commessi i reati di cui agli artt. 493-*ter* c.p., 493-*quater* e 640-*ter* c.p. aggravato dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale. Nel fare questo il legislatore italiano ha adempiuto agli obblighi previsti dall'art. 10 della menzionata direttiva, che impone agli Stati membri di adottare le misure necessarie affinché le persone giuridiche siano ritenute responsabili dei fatti illeciti richiamati dalla direttiva. Sebbene non si possa che accogliere favorevolmente l'introduzione del nuovo art. 25-*octies*.1, risulta di difficile comprensione la motivazione per la quale il legislatore non abbia semplicemente inserito la fattispecie base di cui all'art. 640-*ter* c.p. nel catalogo dei reati presupposto, come sarebbe stato auspicabile. Tuttavia, dal momento che la nuova circostanza aggravante finisce fondamentalmente per coincidere con l'evento della fattispecie base, si potrebbe ritenere che la frode informatica ora rientri sostanzialmente nel catalogo dei reati presupposto. Dunque, una modifica in tal senso risulterebbe ormai soltanto un *pro forma*.

Inoltre, al co. 2 dell'art. 25-*octies*.1 cit. è stato previsto un nuovo illecito amministrativo sussidiario in caso di commissione di ogni altro delitto contro la fede pubblica, contro il patrimonio o che comunque offende il patrimonio previsto dal codice penale, avente ad oggetto gli strumenti di pagamento diversi dai contanti. Poiché la frode informatica è un reato contro il patrimonio e per la sua struttura ha necessariamente ad oggetto strumenti di pagamento diversi dai contanti, a maggior ragione si può ritenere che quest'ultima ipotesi sia a tutti gli effetti oggi ricompresa nel catalogo dei reati presupposto per la responsabilità amministrativa da reato degli enti.

L'allargamento dei reati presupposto per la responsabilità da reato degli enti alla gran parte dei reati informatici e cibernetici è senz'altro da accogliere con favore, dato che in linea di principio ha l'indubbio pregio di rafforzare ulteriormente la tutela penale in materia. Tuttavia, si evidenzia che i reati cibernetici descritti nel corso del presente lavoro quasi mai sono commessi nell'interesse o a vantaggio di enti, società o imprese che svolgono attività economica lecita, quanto, piuttosto, da associazioni a delinquere. È vero che l'ente di cui al d.lgs. 231/2001 può essere stabilmente utilizzato allo scopo unico o prevalente di consentire o agevolare la commissione di reati, come previsto dall'art. 16, co. 3, ma è comunque un qualcosa di diverso rispetto ad un'associazione a delinquere. Certamente, vi possono essere dei casi in cui viene commesso un accesso abusivo al sistema informatico dell'azienda concorrente allo scopo di ottenere i nominativi di clienti, fornitori, dati in merito alla produzione, ecc. o un danneggiamento del sistema informatico di quest'ultima. Tuttavia, nella quasi totalità dei casi, i reati analizzati nel presente lavoro vengono commessi da vere e proprie associazioni a delinquere, non da "enti" ai sensi del d.lgs. in esame. Peraltro, appare

difficile che frodi informatiche e/o le falsificazioni di strumenti di pagamento diversi dai contanti vengano commesse nell'interesse di un'azienda ed ecco, forse, il vero motivo per cui la frode informatica nella sua ipotesi base non è mai stata inserita nel catalogo dei reati presupposto. Non sembra, dunque, che l'inserimento dei reati informatici e cibernetici contro il patrimonio in senso lato nel catalogo di cui al d.lgs. n. 231/2001 sia uno strumento significativo per la repressione degli illeciti in questione, come dimostrato, peraltro, dalla scarsa applicazione che hanno avuto le norme in questione.

Molto più rilevante, invece, è l'inserimento tra i reati presupposto di cui all'art. 24-*bis* quello di cui all'art. 1 co. 11 del d.l. 105/2019, così come convertito dalla l. 18 novembre 2019, n. 133, che sanziona coloro che in occasione degli "incidenti rilevanti" che hanno coinvolto il sistema informatico fornisca informazioni, dati o elementi di fatto non rispondenti al vero od ometta di comunicare entro i termini prescritti i predetti dati, informazioni o elementi di fatto[55]. Le imprese, infatti, tendono a nascondere di aver subìto un attacco informatico, per il timore della pubblicità negativa. Ma è proprio grazie a tale attacco che spesso i criminali informatici riescono ad ottenere un gran numero di dati da vendere sul *darkweb*.

Forse, dunque, sarebbe opportuno un ripensamento del sistema e prevedere ulteriori sanzioni sul modello di quella di cui sopra, per enti quali banche, istituti finanziari e/o imprese, legate al mancato rispetto degli obblighi di segnalazione degli attacchi informatici nonché alla mancata adozione di misure di sicurezza adeguate per i loro sistemi. Infatti, molti siti di *e-commerce* di diverse aziende non rispettano gli standard minimi di sicurezza, né richiedono il secondo fattore di autenticazione. Prevedere, dunque, un'autonoma responsabilità per quegli enti che con la loro negligenza agevolano la commissione di reati informatici servirebbe senz'altro a responsabilizzarli in merito alla necessità di adottare sempre adeguate ed aggiornate misure di sicurezza contro gli attacchi informatici. Per quanto riguarda, poi, specificamente le Banche, potrebbe essere estremamente efficace l'adozione di protocolli di cooperazione con l'Autorità giudiziaria, la quale potrebbe avvalersi dei dati raccolti dai centri per la sicurezza di cui ciascun istituto di credito è dotato e risalire così in tempi più rapidi agli indirizzi IP (e, quindi, all'identità degli utilizzatori) da cui sono partiti gli attacchi informatici.

La cooperazione del settore privato è non solo fondamentale per garantire la sicurezza cibernetica e per prevenire gli attacchi informatici, ma può essere anche

[55] PICOTTI L., *Cybersecurity: quid novi?*, cit., p. 14.

estremamente utile per individuare i responsabili degli attacchi informatici. Si potrebbero, dunque, prevedere incentivi per le aziende particolarmente all'avanguardia come standard di sicurezza informatica, nonché per quelle che si sono dimostrate particolarmente solerti nella segnalazione degli attacchi e siano state collaborative con le Autorità pubbliche, sul modello del c.d. *rating di legalità*, per invogliare anche quelle imprese che non ritengono di investire nella cybersicurezza a farlo.

5. Proposte per un miglior coordinamento delle norme incriminatrici *lato sensu* patrimoniali

Come evidenziato nei capitoli precedenti, vi è un'oggettiva difficoltà per gli interpreti nell'individuare quali siano i rapporti tra le tante fattispecie che vengono in rilievo in occasione della commissione di un reato informatico e, dunque, stabilire quando vi sia concorso effettivo di reati e quando, invece, vi sia concorso apparente di norme. Il sistema dei reati informatici e cibernetici contro il patrimonio *lato sensu*, infatti, è caratterizzato da una moltitudine di fattispecie incriminatrici volte a sanzionare le diverse fasi di un attacco informatico, che nella maggior parte dei casi prevedono una lunghissima lista di condotte, dalle cinque di cui al danneggiamento informatico ex art. 635-*bis* c.p. alle otto di cui all'art. 493-*quater* c.p., e spesso sono in tutto e per tutto simili tra loro, differenziandosi tra loro unicamente per il riferimento al fine perseguito dall'agente.

In molti casi tra i diversi reati vi è una vera e propria progressione criminosa, ma è difficile concludere per l'applicabilità di uno solo di essi. Questo perché la giurisprudenza prevalente delle Sezioni Unite supporta un criterio monistico, basato esclusivamente sul rapporto strutturale tra norme ed esclude così l'utilizzabilità di criteri diversi da quello legislativo di specialità[56]. Ma in questi casi è difficile individuare un rapporto di specialità, sia per la diversità strutturale delle norme, sia perché molte fattispecie si consumano in tempi fisiologicamente differenti. Inoltre, nonostante sia vero che, come sottolineato recentemente anche dalle Sezioni Unite[57], il principio di specialità non può finire per abrogare la disciplina del reato complesso, tra le diverse fattispecie in esame è assai arduo individuare quale tra le tante incriminazioni un reato complesso che assorba in sé il disvalore di tutte le altre

[56] Cass. pen., sez. un., 23 febbraio 2017, n. 20664 e Cass. pen., sez. un., 12 settembre 2017, n. 41588, con nota di SERRA G., *Le Sezioni Unite e il concorso apparente di norme, tra considerazioni tradizionali e nuovi spunti interpretativi*, in *Dir. pen. cont.*, 2017, n. 11, p. 173 ss. In senso conforme anche Cass. pen., sez. un., sentenza 28 ottobre 2010, n. 1963; Cass. pen., sez. un., sentenza 28 ottobre 2010, n. 1235; Cass. pen., sez. un., sentenza 19 aprile 2007, n. 16568; Cass. pen., sez. un., 20 dicembre 2005, n. 47164; Cass. pen., sez. un., sentenza 9 maggio 2001, n. 23427; Cass. pen., sez. un., sentenza 28 marzo 2001, n. 22902.
[57] Cass. pen., sez. un., sentenza 26 ottobre 2021, n. 38402.

fattispecie. Questo anche perché, a seguito di entrambe le novelle legislative qui esaminate, sono state aumentate le pene edittali: perciò, a parte i reati di cui agli artt. 615-*quater* e 493-*quater* c.p., che effettivamente hanno un trattamento sanzionatorio meno severo, che consente di operare un assorbimento, le altre fattispecie esaminate hanno tutte un trattamento sanzionatorio simile.

Si aggiunga poi che l'art. 617-*quater* c.p. prevede una pena superiore nel minimo alle fattispecie base di frode informatica, a quella dell'art. 493-*ter* c.p. e, soprattutto, a quella dell'art. 615-*ter* c.p., al pari dell'art. 617-*quinquies* c.p., che punisce condotte prodromiche alla realizzazione dell'accesso abusivo al sistema informatico, della frode informatica o della falsificazione di strumenti di pagamento. Dunque, proprio perché non appare possibile operare alcun assorbimento, né ritenere si sia in presenza di un reato complesso ai sensi dell'art. 84 c.p., una volta escluso il rapporto di specialità non vi è altra soluzione che ritenere che le fattispecie elencate debbano tra loro concorrere.

È vero però che per il reato di frode informatica sono previste due circostanze aggravanti che innalzano notevolmente il trattamento sanzionatorio della fattispecie base. Tuttavia, la prima circostanza aggravante, rappresentata dal trasferimento di denaro o valuta virtuale, prevede una pena identica rispetto a quella dell'art. 493-*ter* c.p., nonché inferiore nel minimo alle fattispecie in materia di intercettazioni informatiche: per cui non si può ritenere possibile nessun assorbimento. Inoltre, per le altre fattispecie punite con pena più mite, quali ad esempio l'accesso abusivo, poiché la circostanza aggravante in questione sostanzialmente coincide con l'evento della frode informatica nella sua ipotesi base non si può ritenere che la stessa comprenda al suo interno tutti gli elementi costitutivi delle altre fattispecie e assorba il disvalore complessivo del fatto.

Diverso discorso si può fare per la circostanza aggravante della frode informatica commessa con furto o indebito utilizzo dell'identità digitale. In quest'ultimo caso, infatti, la pena prevista è superiore a quelle di tutte le fattispecie poste sia a tutela della riservatezza informatica, sia in materia di intercettazioni informatiche, mentre il concetto di "furto o indebito utilizzo dell'identità digitale" effettivamente sembra richiamare l'abuso delle credenziali di autenticazione e, quindi l'accesso abusivo e/o l'intercettazione delle comunicazioni informatiche. Così interpretato, dunque, l'art. 640-*ter* co. 3 c.p. potrebbe effettivamente costituire un reato complesso idoneo ad assorbire in sé il disvalore delle altre fattispecie menzionate. Tuttavia, si rammenta, il concetto di "furto o indebito utilizzo di identità digitale" non è definito, per cui rimangono ancora incerti i limiti e la portata applicativa di questo elemento. Si potrebbe, infatti, obiettare che il furto d'identità digitale,

coincidendo con l'impersonificazione, in realtà sanzionerebbe semplicemente il fatto di "fingersi" altri soggetti nell'effettuare la disposizione patrimoniale in luogo del soggetto passivo e, in questo modo, negare che la stessa assorba il disvalore delle fattispecie poste a tutela della riservatezza informatica.

La questione dell'individuazione dei rapporti tra le diverse fattispecie, dunque, è ben lungi dal trovare una soluzione univoca. In tale contesto l'art. 81 c.p. assume un ruolo chiave, perché consente di mitigare il trattamento sanzionatorio, che altrimenti sarebbe sproporzionato e, come auspicato da una parte della dottrina[58], in alcuni casi si potrebbe persino operare il c.d. aumento zero.

Al fine di evitare irragionevoli ed ingiustificate duplicazioni sanzionatorie si dovrebbe pertanto procedere ad un profondo e meditato riordino della materia, anche tramite l'abrogazione di qualche fattispecie. Le soluzioni possibili sono diverse, tra cui l'inserimento delle clausole di sussidiarietà per fattispecie quali gli artt. 615-*quater*, 615-*quinquies* e 617-*quinquies*, che sanzionano atti preparatori alla commissione di più gravi reati; oppure una riformulazione di alcune circostanze aggravanti ora esistenti, in modo che sia chiaro che la fattispecie posta a tutela del patrimonio costituisca reato complesso. Si può prendere quale l'esaminata circostanza aggravante del furto o indebito utilizzo dell'identità digitale di cui all'art. 640-*ter*, co. 3, c.p., invece di utilizzare un concetto indefinito, suscettibile di interpretazioni contrastanti, sarebbe più opportuno prevedere una circostanza aggravante speciale per il fatto commesso tramite accesso abusivo al sistema informatico o telematico o, meglio ancora, tramite abuso delle credenziali altrui. In questo modo sarebbe palese il rapporto di specialità della fattispecie aggravata da una tale circostanza rispetto alle altre poste a tutela della riservatezza informatica.

Altra soluzione, anche se più difficilmente praticabile, potrebbe essere quella di ripensare la disciplina generale del concorso apparente di norme, prevedendo espressamente la possibilità di utilizzo di altri criteri oltre a quello della specialità. In prospettiva comparata si evidenzia che il codice penale spagnolo, che regola espressamente il concorso apparente di norme all'art. 8 e, a differenza dell'art. 15 del codice penale italiano, menziona espressamente, tra i criteri guida, non solo il principio di specialità, ma anche quelli di sussidiarietà, di consunzione e di "alternatività" (*alternatividad*). Neppure tale modello è però ritenuto pienamente soddisfacente, tanto che nella dottrina spagnola vi è chi, sottolineando le difficoltà che si incontrano sia nell'ordinamento spagnolo che in quello

[58] SOTIS C., *Il ''concorso materiale apparente'': confine tra artt. 15 e 81 c.p.*, in *Giur. It.*, 2020, n. 1, p. 189 ss., p. 193.

italiano, i quali regolano entrambi più o meno espressamente il concorso di reati, nel definire i rapporti tra le diverse fattispecie, propone quale soluzione di non regolare affatto in via normativa il concorso di norme e di reati, ma di lasciare che sia la prassi giurisprudenziale a decidere di volta in volta quale criterio seguire[59]. Questa soluzione non sembra accettabile, perché serve almeno un criterio definito in via legislativa che orienti il giudice nella sua decisione, pena un *vulnus* del principio di legalità. Se il giudice fosse libero di scegliere in autonomia quali criteri utilizzare per l'individuazione dei rapporti tra le singole fattispecie, sorgerebbero anche problemi con riferimento al principio di uguaglianza, data l'ingiustificata disparità di trattamento rispetto a fatti identici, poiché per un fatto il giudice potrebbe ritenere assorbito un fatto nell'altro e applicare un solo reato, mentre in un altro caso identico potrebbe decidere di utilizzare il solo criterio della specialità e condannare il reo per più reati. Dunque, neppure la previsione di tanti diversi criteri sembra essere una soluzione adeguata. Piuttosto che rendere il sistema più caotico con l'aggiunta di ulteriori criteri, sarebbe più efficace intervenire direttamente sulla disciplina del reato continuato, prevedendo che nei casi di progressione criminosa si applichi unicamente la fattispecie più grave, sul modello del § 52 StGB tedesco. Questa scelta consentirebbe di correggere le storture del sistema, nascenti da casi in cui il legislatore abbia introdotto dei veri e propri "doppioni" senza regolare espressamente il rapporto tra le fattispecie mediante l'utilizzo di clausole di sussidiarietà espressa. Tuttavia, poiché il problema è sentito in modo particolare per i reati cibernetici sopra esaminati, non si ritiene necessario cambiare *in toto* la norma di cui all'art. 81 co. 2 c.p. per assimilarla alla *Tateinheit*, ma si può benissimo creare una disciplina autonoma e derogatoria specifica per questi ultimi, sul modello del vecchio art. 219 l. fall. per la pluralità di fatti di bancarotta in concorso tra loro, previsione ora contenuta nell'art. 326 del Codice della crisi d'impresa.

6. Riflessioni conclusive tra necessità di prevenzione, cooperazione internazionale e migliore qualità del sistema normativo per una più efficace tutela (non solo penale) del patrimonio

Le ricerche sugli attacchi informatici dimostrano come siano le persone ad essere l'anello debole della catena della sicurezza informatica e a costituirne la vulnerabilità principale. In molti casi, infatti, è proprio grazie alla scarsa cultura ed attenzione in materia

[59] SUÁREZ GONZÁLEZ C., *Concurso de delitos: propuesta de regulación con vista a un Código penal europeo*, in K. Tiedemann, A. Nieto Martín (a cura di), *Eurodelitos. El derecho penal económico en la Unión Europea*, Cuenca, 2003, p. 59 ss., p. 62.

di *cybersecurity* che i criminali informatici riescono ad introdursi nei sistemi informatici di aziende e privati. Dunque, un elemento fondamentale nella lotta ai reati cibernetici contro il patrimonio *lato sensu* è senz'altro la prevenzione: un'efficace sistema di sicurezza informatica è il primo elemento che funge da deterrente alla criminalità informatica[60].

In questi ultimi anni molto è stato fatto in tal senso e le campagne volte a sensibilizzare gli utenti sui rischi del *web* sono sempre più numerose e capillari. Diversi istituti bancari aggiornano periodicamente i clienti in merito alle nuove minacce informatiche *online* e li informano della necessità di non comunicare mai a nessuno i loro codici personali. Un ruolo importante è svolto anche dai *social media*, anche della Polizia postale, sui quali è possibile trovare molte notizie in merito alle tecniche utilizzate dai criminali informatici nonché numerosi consigli su come difendersi. Questo è senz'altro da accogliere con favore, perché l'accrescimento della consapevolezza degli utenti nell'utilizzo dei nuovi strumenti di pagamento comporta un minor rischio per gli stessi di divenire vittime di questi reati.

Anche il legislatore europeo ha compreso l'importanza di prevedere ulteriori disposizioni rispetto a quelle strettamente penali, che sono fondamentali nella repressione degli attacchi informatici contro il patrimonio, in particolare in merito alla raccolta di dati statistici per effettuare un efficace monitoraggio. Oltre agli specifici provvedimenti in materia di *cybersecurity* già analizzati, infatti, sia la direttiva 2013/40/UE che la direttiva 2019/713/UE prevedono delle disposizioni in merito allo scambio di informazioni tra i diversi punti di contatto operativi nazionali con riferimento ai reati menzionati nelle direttive stesse, nonché in merito al loro monitoraggio e alle relative statistiche. L'art. 16 della direttiva 2019/713/UE poi, intitolato "assistenza e sostegno alle vittime", prevede specificamente l'obbligo per gli Stati membri di prevedere appositi sistemi per fornire assistenza e supporto alle vittime di frodi e falsificazioni di strumenti di pagamento diversi dai contanti. Queste disposizioni sono significative nonché estremamente utili, perché la raccolta dei dati in merito agli attacchi informatici aiuta le Autorità pubbliche ad avere una chiara comprensione della portata del fenomeno.

Il d.lgs. 184/2021 di attuazione della direttiva 2019/713/UE, oltre ad aggiungere e modificare le fattispecie penali esaminate, ha introdotto altresì diverse disposizioni, che pur avendo natura extra-penale, hanno notevole rilevanza, perché volte a garantire un'efficace cooperazione internazionale nel contrasto ai reati commessi contro gli strumenti di

[60] Così ITU, *Understanding Cyber crime*, cit.

pagamento diversi dai contanti. Infatti, l'art. 4 prevede la raccolta di dati statistici sulle frodi e sulle falsificazioni relative a strumenti di pagamento diversi dai contanti. In particolare, si prevede la raccolta di dati relativi al numero dei procedimenti iscritti e dei procedimenti definiti con sentenza di condanna per reati aventi ad oggetto strumenti di pagamento diversi dai contanti, nonché al numero delle persone indagate e al numero delle persone condannate per i medesimi reati. Questa è una disposizione significativa, perché ad oggi nelle statistiche giudiziarie le frodi informatiche vengono conteggiate assieme alle truffe comuni, mentre i reati di indebito uso e falsificazione di carte di credito e di pagamento non sono neppure inseriti in una categoria a sé stante, bensì indicati alla voce "*altri reati*"[61]. La raccolta di specifici dati aggiornati consente invece il loro scambio con organismi quali la Commissione europea, Europol ed Eurojust, anche ai fini di una miglior cooperazione tra i diversi Stati membri. Proprio a tal fine il successivo art. 5 del d.lgs. cit. individua nella Sala operativa internazionale, incardinata nel Servizio per la cooperazione internazionale di polizia della Direzione centrale della polizia criminale, il punto di contatto operativo nazionale per lo scambio di informazioni raccolte e richieste dalle autorità di altro Stato membro relative ai reati di cui al nuovo decreto.

Non si comprende, però, perché il nostro legislatore non abbia previsto una simile disposizione anche in occasione dell'attuazione della direttiva 2013/40/UE. L'art. 19 della l. 23 dicembre 2021, n. 238, infatti, diversamente da quanto imposto dalla menzionata direttiva, non ha previsto alcuna disposizione in merito allo scambio di informazioni tra le autorità degli Stati membri e alla redazione di statistiche sull'incidenza dei reati di cui alla direttiva. La raccolta delle informazioni e statistiche, dunque, oggi è prevista unicamente per i reati relativi alle frodi e falsificazioni di strumenti di pagamento diversi dai contanti. Nulla, invece, per quanto riguarda i reati relativi agli attacchi contro i sistemi di informazione. Quest'ultima lacuna è da correggere quanto prima, perché solo prevedendo un efficace sistema di monitoraggio in merito agli attacchi informatici contro i sistemi di informazione è possibile avere un quadro completo del fenomeno e predisporre o adeguare le strategie di contrasto. Inoltre, la mancanza di dati disponibili in merito agli attacchi informatici rende la cooperazione internazionale più ardua (se non impossibile).

Come evidenziato più volte nel corso del presente lavoro, il *cybercrime*, macrocategoria che ricomprende anche gli attacchi informatici diretti contro il patrimonio,

[61] V. dati dell'Istituto Nazionale di statistica relativi all'anno 2019 con riguardo alla tipologia di reati commessa, ai delitti di cui si è scoperto l'autore e dei condannati con riferimento alla natura del reato, disponibili *online* al sito «http://dati.istat.it».

è un fenomeno transnazionale. Il criminale informatico, infatti, può agire da remoto, senza muoversi dal suo Paese, utilizzando esclusivamente la rete *Internet*. Per cui in moltissimi casi reo e vittima si trovano fisicamente distanti anche centinaia o migliaia di chilometri. Ciò non è affatto indifferente per il diritto penale. Il fatto che il *web* sia privo di qualcosa di vagamente assimilabile ai confini nazionali pone evidenti problemi anche di giurisdizione. Oggi i reati informatici e cibernetici sono perseguiti dai diversi giudici nazionali, ma vi è chi propone l'istituzione di una Corte penale internazionale per il *cyberspace*, la cui giurisdizione sarebbe riservata ai *cybercrimes* con maggiore rilevanza, tra cui la violazione di trattati internazionali in materia di *cybercrime*, nonché gli attacchi *cyber* diretti contro le infrastrutture critiche di un Paese[62]. Vi è chi, invece, propone di attribuire alla già esistente Corte Penale Internazionale la giurisdizione sui reati cibernetici più gravi, quali ad esempio la violazione su larga scala della proprietà intellettuale, la pornografia informatica, le frodi informatiche o gli attacchi informatici commessi su scala internazionale, a seconda dell'estensione territoriale della condotta e della sua gravità, che permetterebbe un miglior coordinamento tra diverse giurisdizioni[63]. Alcuni studiosi ritengono che già rientrino nella competenza della Corte Penale Internazionale quelle ipotesi di illeciti commessi tramite mezzi informatici sussumibili nelle fattispecie previste dallo Statuto di Roma o dirette a ledere sistemi informatici di importanza primaria per l'ordine pubblico internazionale o di altri Stati[64]. Ad oggi, però, non vi è notizia di casi di sabotaggio informatico giudicati da quest'organo sovranazionale.

Effettivamente un'idea potrebbe essere quella di ampliare la Convenzione *Cybercrime*, che nel corso degli anni ha visto moltiplicare le adesioni da parte dei diversi Stati, prevedendo qualcosa come un terzo protocollo addizionale, con l'istituzione di una Corte competente a giudicare sui reati cibernetici più gravi in conformità alla Convenzione stessa. Tuttavia, non è detto che tale scelta possa essere accolta con favore dalla maggioranza degli Stati aderenti, perché costituirebbe un'importante rinuncia alla sovranità nazionale. Se, dunque, com'è prevedibile, ad aderire a tale proposta fossero unicamente pochi Stati, il progetto sarebbe destinato a naufragare, dato che non è pensabile che una Corte possa operare in collaborazione con pochi Stati e, soprattutto, diversi rispetto a quelli aderenti. Va evidenziato che le condotte dei reati informatici, anche qualora assumano rilevanza

[62] WEISSBRODT D., *Cyber-Conflict, Cyber-Crime, and Cyber-Espionage*, in *Minn. J. Int'l L.*, 2013, vol. 22, n. 2, p. 347 ss., p. 369.
[63] FLORES PRADA I., *Criminalidad informática*, cit., p. 316 s.
[64] CAMPLANI F., Locus commissi delicti, cit., p. 26.

transnazionale, generalmente non assumono rilievo paragonabile a quello dei crimini previsti dalle norme penali internazionali, né riguardano un insieme di soggetti passivi del medesimo ordine di grandezza[65]. La soluzione relativa all'istituzione di un'unica Corte penale internazionale, dunque, non appare allo stato praticabile.

Soluzione più realistica e attuabile sarebbe quella di inserire nelle Convenzioni internazionali, a partire dalla Convenzione *Cybercrime*, regole comuni e precise in materia di giurisdizione per i reati cibernetici, adeguate al mutato contesto tecnologico, nonché meccanismi di risoluzione di eventuali conflitti di giurisdizione tra gli Stati aderenti. L'Unione Europea potrebbe, da questo punto di vista, essere pioniera ed eliminare il riferimento al "luogo del commesso reato" per dare centralità ai criteri della residenza della vittima nonché della collocazione dei server oggetto di attacco informatico.

Più che istituire una vera e propria Corte penale, si ritiene molto più utile rafforzare ed estendere i diversi strumenti di cooperazione internazionale esistenti tra le autorità investigative e giudiziarie, direzione verso la quale, peraltro, va l'adozione del secondo protocollo addizionale alla Convenzione *Cybercrime,* volto a rafforzare la cooperazione internazionale nella raccolta e divulgazione delle prove elettroniche.

Va però evidenziato che, per attivare e rendere possibile la cooperazione internazionale, è necessario che la legge penale sostanziale risponda a determinati requisiti. A tal proposito, come evidenziato nei capitoli precedenti, il nostro sistema di reati informatici e cibernetici contro il patrimonio *lato sensu* è caratterizzato da una moltitudine di fattispecie incriminatrici che in certi casi sanzionano comportamenti di per sé neutri e con pene troppo basse per giustificare l'attivazione di strumenti di cooperazione internazionale. Sono proprio alcune delle condotte sanzionate da queste fattispecie c.d. minori, tra cui *in primis* la vendita di dati illecitamente carpiti, che necessitano maggiormente di una pena elevata in grado di giustificare l'attivazione degli strumenti di cooperazione internazionale. Si è, infatti, più volte ribadita la pericolosità del fenomeno del *Cybercrime-as-a-service*, che ha mutato notevolmente la struttura degli attacchi informatici contro il patrimonio e dietro cui operano associazioni a delinquere di carattere transnazionale. Ma le fattispecie esaminate, nonostante il loro elevato numero, non appaiono allo stato adeguate a reprimere il fenomeno criminoso in questione.

Il problema non riguarda unicamente la legislazione italiana, ma anche quella tedesca e spagnola. In questo particolare settore, infatti, la legislazione europea svolge un ruolo

[65] *Ibid.*

centrale, obbligando i legislatori nazionali ad attuare nel codice penale decisioni prese da organi europei. Il dettato europeo tende ad essere capillare, onnicomprensivo, nel tentativo di tenere il passo con l'evoluzione delle tecniche utilizzate dai criminali informatici. A tal fine, prevede lunghe liste di condotte, spesso di significato identico o comunque molto simile (basti pensare al "cancellando" e al "sopprimendo" di cui all'art. 6 della direttiva 2019/713/UE), che poi i legislatori devono obbligatoriamente sanzionare. Per quanto riguarda specificamente la punibilità degli atti preparatori, vengono raggruppate numerose condotte assolutamente eterogenee, tra cui anche condotte non adatte all'universo virtuale, come ad esempio "l'importazione" e il "trasporto" di dati informatici, che in molti casi non possono neppure essere definiti "atti preparatori". Spesso, poi, le direttive esaminate sostituiscono precedenti Decisioni quadro, di cui viene integralmente trasposto il testo nella nuova direttiva, con qualche piccola modifica, che spesso i legislatori nazionali non sono in grado di individuare.

Come si è avuto modo di verificare, il risultato della stratificazione normativa e del numero elevatissimo di condotte che le direttive obbligano a sanzionare, con la possibilità di incorrere in una procedura di infrazione, è che in quest'ambito i legislatori nazionali hanno fatto un largo uso della c.d. legislazione simbolica. Essa, in questi casi specifici, al posto di essere utilizzata per accontentare le istanze sociali[66], viene utilizzata per evitare procedure di infrazione per mancata attuazione delle direttive comunitarie. Esempi paradigmatici sono il sopra esaminato § 152c dello *Strafgesetzbuch* tedesco, la recente aggiunta delle numerose condotte sanzionate nella *estafa informática* spagnola, nonché la circostanza aggravante dell'avvenuto trasferimento di denaro, valore monetario o valuta virtuale introdotta nella frode informatica italiana. Di tutte queste modifiche non vi era assolutamente necessità. I legislatori nazionali, però, per evitare o chiudere procedure di infrazione aperte dalla Commissione, hanno preferito aggiungere oggetti, condotte, ecc. alle fattispecie già in vigore o introdurne di nuove, ad esempio l'artt. 493-*ter* c.p. e il § 152c StGB, rendendo il quadro normativo in tutti e tre gli ordinamenti assolutamente sovrabbondante. Spesso, addirittura, la norma nazionale ricalca pedissequamente il testo della direttiva.

Dato che in tutti e tre gli ordinamenti erano già presenti da tempo reati informatici contro il patrimonio, con le ultime riforme tutti e tre i legislatori si sono concentrati prevalentemente sui reati prodromici alla commissione di più gravi reati informatici e/o cibernetici, aggiungendo condotte a quelle già sanzionate o, in alcuni casi, introducendo

[66] DÍEZ RIPOLLÉS J.L., *La racionalidad de las leyes penales. Practica y teoría*, Madrid, 2013, p. 74.

nuove norme penali che costituiscono veri e propri "doppioni". La tendenza all'onnicomprensività di queste fattispecie, che nella maggior parte dei casi sanzionano condotte neutre, viene compensata dalle bassissime pene in esse previste, con la sola eccezione di alcune, non tutte, fattispecie spagnole. Il risultato è che le norme in questione hanno trovato scarsissima applicazione, come dimostrano le pochissime pronunce giurisprudenziali.

Sanzionare un elevato numero di condotte di per sé neutre, ma con pena mite, mal si concilia con l'esigenza di razionalità della legge penale, né aiuta la coerenza del sistema. Il diritto penale, infatti, deve limitarsi a sanzionare le condotte che sono gravemente pregiudizievoli per i beni giuridici tutelati. Prevedere una pena bassa per condotte di minore importanza non è sufficiente ad evitare la lesione del principio di frammentarietà. È poi la gravità delle condotte che giustifica l'intervento penale, non si può utilizzare lo stesso identico mezzo per aggressioni al bene giuridico intollerabili e per quelle di minore importanza[67]. Del resto, la creazione di innumerevoli fattispecie "doppione" punite con pene piuttosto miti non aiuta certo la cooperazione internazionale e la repressione di fenomeni criminosi complessi come il *Cybercrime-as-a-service*.

L'unica soluzione veramente efficace sarebbe un nuovo intervento di completo riordino della materia, anche da parte del legislatore europeo, il quale dovrebbe, innanzitutto, individuare in modo chiaro la differenza tra la frode informatica e la falsificazione e indebito utilizzo di strumenti immateriali diversi dai contanti. Dopodiché si dovrebbero assolutamente rivedere i lunghi elenchi di condotte ed eliminare quelle che hanno identico significato e/o mal si adattano alla realtà virtuale. Sarebbe infine opportuno distinguere tra condotte che costituiscono veri e propri atti preparatori per ulteriori reati informatici e quelle che, invece, rappresentano autonome manifestazioni criminose, una su tutte la vendita di dati, prevedendo diverse sanzioni adeguate alla mutata realtà fenomenica.

[67] DÍEZ RIPOLLÉS J.L., *La racionalidad*, cit., p. 142.

Conclusioni

Nel presente elaborato si è evidenziato come gli attacchi informatici contro il patrimonio costituiscano un fenomeno in rapida espansione e in continua evoluzione, che non coinvolge solo privati ed aziende, ma anche infrastrutture critiche dello Stato. Inoltre, negli ultimi anni sono state perfezionate tecniche sempre più sofisticate, in modo da rendere i *malware* non individuabili dai sistemi antivirus, ed è anche mutato il profilo dei criminali informatici. Questi ultimi, infatti, oggi si possono dividere in due categorie: coloro che, esperti in informatica, si dedicano alla creazione di *ransomware*, *spyware*, ecc. per poi venderli sul *web* e gli acquirenti di tali prodotti, che sono coloro che poi effettivamente ne fanno utilizzo. In molti casi i soggetti di entrambe le categorie sono componenti di associazioni a delinquere, che possono operare su scala internazionale. Oltre a tali soggetti vi sono poi i *money mule*, che come interposti si occupano di mascherare l'origine illecita dei profitti ottenuti sia da coloro che hanno venduto il *malware* o le credenziali altrui, sia da coloro che hanno effettivamente compiuto l'attacco informatico.

Nel corso del tempo, pertanto, è diventata sempre più evidente l'esigenza di proteggere le infrastrutture informatiche pubbliche e private dalle minacce dirette a ledere non solo il patrimonio, ma anche la loro l'integrità. Sono, per questo, state adottate diverse iniziative congiunte a livello sovranazionale, sia a livello europeo che internazionale, sulla base delle quali il nostro legislatore ha dapprima introdotto nuove fattispecie incriminatrici volte a sanzionare i nuovi fenomeni criminosi, ed in seguito ha provveduto a modificarle per adeguarle a quanto stabilito in sede internazionale.

Il sistema dei reati informatici e cibernetici contro il patrimonio, dunque, è composto da una molteplicità di fattispecie, tra le quali alcune includono al loro interno elementi tecnico-informatici senza i quali non sarebbero neppure concepibili, mentre altre sono fattispecie tradizionali che, seppur non presentando le menzionate caratteristiche tecnico-informatiche tra i loro elementi costitutivi, possono comunque essere commesse *online*. Inoltre, come si è avuto modo di evidenziare nel corso del presente lavoro, gli attacchi informatici diretti contro il patrimonio non ledono unicamente quest'ultimo, ma anche altri beni giuridici, quali la riservatezza informatica e l'integrità di dati e sistemi informatici. Ai reati contro il patrimonio in senso stretto, dunque, si aggiungono altre fattispecie che sanzionano condotte prodromiche alla commissione di reati informatici e cibernetici contro il patrimonio.

Mentre fino a poco tempo fa si poteva ritenere che nell'ambito applicativo delle fattispecie in vigore non rientrassero tutte le fasi dei nuovi fenomeni criminosi diretti contro il patrimonio sul *web*, a seguito delle ultime riforme è emerso il contrario. Infatti, come si è esaminato, in caso di attacco informatico diretto a ledere il patrimonio è applicabile almeno una fattispecie. Non solo nel nostro ordinamento, ma anche in quello tedesco e spagnolo si può osservare la tendenza alla capillarità della legislazione penale di contrasto al *cybercrime*, che aspira a sanzionare ogni singolo comportamento o atto preparatorio che possa essere rilevante con riferimento agli attacchi informatici, nel difficile tentativo di "rincorrere" i criminali informatici. Nonostante questo sforzo, neppure oggi le norme incriminatrici possono essere ritenute realmente in grado di reprimere tutti gli attacchi informatici contro il patrimonio. Questo perché sono ancora legate a vecchi schemi e si basano sulla tradizionale idea di *hacker*, come soggetto dotato di medie o elevate competenze informatiche che compie da solo tutte le fasi dell'attacco informatico, dalla costruzione del *malware* alla manipolazione del sistema informatico della vittima. Tuttavia, come si è dato conto nella presente analisi, così ora non è e, di riflesso, le fattispecie non risultano adeguate al mutato contesto. Nella maggior parte dei casi, infatti, colui che materialmente accede al sistema *home banking* della vittima non ha nessuna particolare competenza informatica, ma si è limitato ad acquistare un *exploit kit*.

Il *cybercrime-as-a-service* è fenomeno molto più pericoloso rispetto ad un prelievo non autorizzato di una somma di denaro da un singolo conto corrente, perché consente alla criminalità informatica di evolversi e diventare fenomeno "di massa". Infatti, è molto più redditizio noleggiare *bootnet* o progettare *malware* da vendere, che effettuare materialmente l'accesso abusivo al conto corrente del correntista e/o utilizzare i dati della sua carta di credito per effettuare acquisti. Inoltre, i rischi sono molto minori, soprattutto per quanto riguarda le sanzioni. Se, infatti, un soggetto si dedica alla vendita dei dati delle carte di credito altrui rischia una pena molto minore rispetto a colui che le acquista e ne fa uso. Tuttavia, è proprio il primo che consente a quest'ultimo di commettere un reato che, altrimenti, non avrebbe neppure le capacità di commettere. In tale contesto, la frode informatica o il *ransomware* ai danni del singolo non sono che la punta dell'iceberg di un sistema molto più complesso, dietro il quale vi sono associazioni a delinquere che si occupano di costruire *malware* da vendere a caro prezzo su larga scala e di occultare l'origine illegale del corrispettivo.

A fronte di questa situazione, la legislazione penale in materia è assolutamente sovrabbondante, con fattispecie di dubbia utilità pratica e che nel corso degli anni sono state

oggetto di pochissime pronunce giurisprudenziali, a riprova della loro scarsa applicazione. Vi sono, infatti, diverse fattispecie che sanzionano l'aggressione al patrimonio vera e propria e un numero elevatissimo di norme che puniscono condotte prodromiche alla commissione di ulteriori reati, anche contro il patrimonio, con pena poco elevata e quindi non sufficiente per attivare gli strumenti di cooperazione giudiziale che, invece, la transnazionalità dei fenomeni imporrebbe. La previsione di una bassa pena, infatti, va a compensare il fatto che le condotte ivi sanzionate sono per la maggior parte neutre e caratterizzate unicamente dalla strumentalità rispetto all'offesa di ulteriori beni giuridici. Questo è dovuto alla convinzione erronea secondo cui tutte le condotte prodromiche ivi sanzionate vengano commesse dallo stesso autore del successivo reato contro il patrimonio, per cui la previsione di identiche sanzioni per tutte le fasi di uno stesso *iter criminis* violerebbe il principio di proporzionalità.

Questa è una tendenza presente soprattutto a livello di normativa UE in materia. La stessa Unione Europea, come si evince dal Considerando n. 13 della direttiva 713/2019/UE auspica che condotte come la raccolta ed il possesso di strumenti di pagamento diversi dai contanti quali il *phishing* e lo *skimming*, siano qualificate come reato a sé stante, evidenziando la necessità che le stesse siano sanzionate indipendentemente dall'effettivo uso degli strumenti di pagamento diversi dai contanti[1]. Tuttavia, poi, quando si tratta di stabilire i fatti che il legislatore nazionale è obbligato a prevedere come reato, il legislatore europeo raggruppa in un unico articolo un lungo elenco di condotte tutt'altro che omogenee, in molti casi prive di disvalore intrinseco e comunque riconducibili a diverse fasi degli attacchi informatici contro il patrimonio, per le quali viene poi individuato un minimo della pena massima più basso, rispetto a quello previsto per gli altri reati contro il patrimonio in senso stretto.

Gli effetti sulle normative nazionali di tale tecnica legislativa sono a loro volta discutibili. Come si è evidenziato, infatti, in tutti gli ordinamenti esaminati ci sono una serie di disposizioni che sanzionano l'aggressione vera e propria al patrimonio ed un'altra serie di disposizioni che incriminano un ampio fascio di condotte di carattere assolutamente

[1] «*Condotte come la raccolta e il possesso di strumenti di pagamento allo scopo di commettere frodi, ad esempio mediante il* phishing, *lo* skimming, *oppure indirizzando o reindirizzando gli utenti di un servizio di pagamento verso siti web falsi, e la loro distribuzione, ad esempio vendendo su Internet informazioni relative alle carte di credito, dovrebbero essere qualificate come un reato a sé stante, indipendentemente dal requisito di un'utilizzazione fraudolenta dei mezzi di pagamento diversi dai contanti. Pertanto, tali condotte criminali dovrebbero includere anche i casi in cui il possesso, l'ottenimento o la distribuzione non portino necessariamente all'utilizzazione fraudolenta di tali strumenti di pagamento. Tuttavia, nei casi in cui la presente direttiva configura il possesso o la detenzione come reato, tale criminalizzazione non dovrebbe comprendere la semplice omissione. La presente direttiva non dovrebbe sanzionare l'uso legittimo degli strumenti di pagamento, anche nel quadro della fornitura di servizi di pagamento innovativi come quelli generalmente messi a punto dalle società di tecnologia finanziaria*».

eterogeneo che hanno ad oggetto dati, *password*, *software*, ecc. che possono essere utilizzati per commettere un reato. Queste condotte sono state raggruppate in diverse fattispecie, in alcuni casi vere e proprie duplicazioni che si differenziano tra loro solo per la finalità perseguita dal soggetto agente, che nell'intenzione del legislatore dovrebbero sanzionare gli atti preparatori alla commissione di futuri reati informatici. Infatti, quando il legislatore prevede espressamente che la condotta venga sorretta dalla speciale finalità di commettere un futuro reato (come avviene per l'art. 493-*quater* del nostro codice penale, per i §§ 202c e 263a dello *Strafgesetzbuch* tedesco e per gli artt. 197-*ter*, 249.2 lett. a) e 400 *Código Penal* spagnolo) o comunque un fatto lesivo (come per i reati di cui agli artt. 615-*quater*, 615-*quinquies*, 617-*quinquies* del nostro codice penale) le condotte incriminate hanno un evidente carattere preparatorio. Il legislatore anticipa la punibilità rispetto alla consumazione di un altro più grave reato, sanzionando condotte che, nel normale decorso criminoso, si collocano in una fase cronologicamente anteriore addirittura rispetto al tentativo di quel secondo reato. Proprio perché si tratta di reati preparatori, essi non possono essere puniti con pena identica o addirittura superiore rispetto al reato consumato, pena il mancato rispetto del principio di proporzionalità in materia penale. Eccezione in tal senso è costituita dall'ordinamento spagnolo, ove gli atti preparatori sono sanzionati con la stessa pena prevista per la fattispecie consumata, cosa che, come si è visto, è tutt'ora oggetto di critiche. Altra eccezione, poi, è presente nel nostro ordinamento proprio all'art. 617-*quinquies* c.p., che, in controtendenza rispetto alle altre fattispecie simili, punisce quelli che nell'intenzione del legislatore costituiscono "atti preparatori" della successiva intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche di cui all'art. 617-*quater* c.p. con una pena identica a quest'ultima fattispecie e particolarmente elevata, se raffrontata con quella delle fattispecie poste a tutela della riservatezza informatica.

Tuttavia, ci si dovrebbe porre la domanda se davvero tutte le condotte sanzionate dalle norme esaminate possano essere classificate come "atti preparatori" della frode informatica, del danneggiamento informatico, ecc. La risposta non può che essere negativa. Si tratta, infatti, di comportamenti eterogenei che presentano un diverso grado di pericolosità e di disvalore sociale. Queste fattispecie sanzionano non solo le attività che l'agente compie per commettere quel successivo determinato reato, ma anche altre tipologie di atti prodromici che non costituiscono atti preparatori in senso stretto, bensì attività che l'agente compie per aiutare un terzo a commettere un reato ovvero semplicemente per agevolarne o facilitarne la commissione. Affermare che il trasporto, il commercio e la messa a disposizione di altri di dati e programmi informatici possano essere considerati "atti

preparatori" di una frode o un danneggiamento informatico sarebbe come ritenere che la vendita illegale di armi possa costituire atto preparatorio rispetto alla commissione di un successivo omicidio. Alcune condotte, quindi, non sanzionano veri e propri atti preparatori, ma sono, invece, riconducibili ai c.d. reati di ostacolo.

L'idea del legislatore spagnolo di punire con la medesima pena del reato consumato gli "atti preparatori", quindi, non è di fondo completamente errata, perché alcune delle condotte ivi sanzionate, quali il trasporto, il commercio e la messa a disposizione di terzi di dati, programmi informatici, o dispositivi idonei a commettere reati non costituiscono atti preparatori, bensì ipotesi tipizzate di concorso di persone nel reato. Né può valere l'obiezione per cui punire "atti preparatori" quali il commercio di dati illecitamente ottenuti, con la stessa pena stabilita per il loro successivo utilizzo, avrebbe un effetto criminogeno, dato che gli studi dimostrano che la vendita di *malware*, reti *bootnet*, ecc. è particolarmente redditizia e coloro che se ne occupano preferiscono assicurarsi sicuri guadagni con limitati rischi di individuazione da parte delle Autorità, piuttosto che utilizzare effettivamente i prodotti da loro venduti, col rischio di essere scoperti.

Il problema nasce dalla mescolanza di condotte eterogenee che effettivamente costituiscono atti preparatori alla commissione della frode informatica, quali il procurarsi, l'ottenere o il fabbricare *malware*, e che, quindi, in ragione del principio di proporzionalità, devono essere sanzionate con pena meno grave del reato consumato, con altre che, invece, non lo sono e costituiscono espressione del diverso e ben più grave fenomeno criminoso del *Cybercrime-as-a-service*. In questo senso appare condivisibile la scelta del legislatore tedesco di sanzionare la c.d. ricettazione di dati con una fattispecie autonoma, ovvero il § 202d StGB. Anche la pena prevista per quest'ultima fattispecie, però, si rivela inadeguata, perché ancorata allo schema tradizionale secondo cui la vendita di dati è condotta caratterizzata da minor disvalore rispetto ai reati informatici consumati contro il patrimonio. Tant'è che il massimo della pena prevista è identico a quello di cui al § 202c StGB, che punisce gli atti preparatori alla commissione di spionaggio e intercettazione di dati, e, dunque, sensibilmente inferiore alla pena prevista per la *Computerbetrug*. Inoltre, vi è la clausola per cui l'autore del reato presupposto non può rispondere anche a titolo di *Datenhehlerei*. Poiché, dunque, il diverso § 202c StGB sanziona proprio colui che si procura, vende, cede, distribuisce, ecc. *password* o *malware*, condotte prodromiche alla realizzazione della ricettazione di dati, il reato applicabile sarà sempre e soltanto il § 202c StGB, dato che per riuscire a divulgare dati è necessario prima procurarseli, salvi casi limite.

Un diritto penale che tenga conto delle nuove fenomenologie emergenti nel nostro tempo dovrebbe considerare la compravendita dei dati, dei *malware* e simili come un atto criminoso a sé stante, non come mero atto preparatorio alla commissione di più gravi reati contro il patrimonio. Del resto, la vendita, la cessione, ecc. di dati e credenziali di autenticazione altrui lede beni giuridici ben più importanti del patrimonio, ovvero, come si è esaminato, la riservatezza informatica, l'identità digitale, ecc., anche e soprattutto tenendo conto del fatto che, come si è visto, non sempre è possibile cambiare i fattori di autenticazione, se ad esempio vengono utilizzati dati biometrici o comunque dati personali quali ad esempio il codice fiscale che non è possibile cambiare.

Andrebbe, dunque, preso atto che il *Cybercrime-as-a-service* costituisce fenomeno criminoso autonomo rispetto ai successivi reati informatici commessi dagli acquirenti di tali "prodotti", riconducibile più al concorso di persone che agli atti preparatori. Occorrerebbe, pertanto, distinguere tra quelle condotte che effettivamente costituiscono atti preparatori alla successiva commissione di un altro più grave reato informatico o cibernetico, quali ad esempio l'acquisto, la costruzione, ecc. di un *malware*, di un *bootkit*, ecc. rispetto a quelle che, invece, si sostanziano nella consapevole "messa a disposizione di terzi" di un programma informatico pericoloso, che possono non essere cronologicamente prossimi all'inizio della condotta tipica. Per cui, al posto di sanzionare con una pena ridotta condotte neutre e di dubbio disvalore penale, quali ad esempio il mero possesso di dati o di *password* altrui, oppure difficilmente riconducibili all'universo "virtuale" quali il trasporto, "l'importazione" e "l'esportazione", sarebbe più opportuno sanzionare direttamente il commercio o lo scambio, con pena adeguata al maggior disvalore di tali condotte, che consenta l'attivazione di efficaci strumenti di cooperazione giudiziale. Quelli che, invece, effettivamente costituiscono atti preparatori, andrebbero sanzionati con pena ridotta e proporzionata rispetto a quella del successivo reato e nella relativa fattispecie sarebbe senz'altro opportuno l'inserimento di una clausola di sussidiarietà espressa, in modo tale da definire in modo chiaro i rapporti con il reato informatico o cibernetico finale, che potrebbe essere costituito anche dalla stessa vendita o ricettazione di dati e programmi informatici dannosi. In questo modo, il ripensamento della struttura complessiva dei reati informatici contro il patrimonio consentirebbe anche di risolvere lo spinoso problema dell'individuazione dei rapporti tra le innumerevoli fattispecie presenti nel nostro ordinamento. Si evidenzia poi che al posto di prevedere due o più fattispecie con identica struttura che sanzionano gli atti preparatori, sarebbe opportuno, anche per ragioni di economia legislativa, prevedere un'unica fattispecie, sul modello del § 202c StGB, che

sanzioni in generale gli atti preparatori alla commissione di più gravi reati informatici e cibernetici.

Questa "bipartizione" tra condotte che costituiscono un contributo materiale alla realizzazione di un concreto fatto illecito commesso da altri e quelle che, invece, costituiscono veri e propri atti preparatori può essere già operata in autonomia dal singolo legislatore nazionale. Le direttive, infatti, si limitano a prevedere l'obbligo per gli Stati di sanzionare i comportamenti criminosi in esse descritti ed a prevedere sanzioni minime non inferiori ad un certo livello, ma nulla vieta al singolo Stato di decidere in autonomia come collocare le diverse condotte in diverse fattispecie e prevedere sanzioni più elevate per quelle che presentano un disvalore maggiore.

La selezione delle condotte che realmente sono idonee a mettere in pericolo il bene giuridico del patrimonio, invece, deve essere attuata in primo luogo dal legislatore europeo, il quale dovrebbe abbandonare la prassi di prevedere lunghi elenchi di condotte dal significato simile e, invece, richiamare solo quelle che presentano il disvalore maggiore. Si ricorda, infatti, che nel sistema la salvaguardia della libertà economica è di primaria importanza, per cui l'ordinamento giuridico deve sì difendere i diritti patrimoniali degli individui, ma senza intervenire dinnanzi a comportamenti leciti. In tale ambito, dunque, vanno selezionate, quali meritevoli di sanzione, solo quelle condotte ritenute particolarmente dannose, perché il principio di frammentarietà serve anche a tutelare la libertà economica.

Questa esigenza è particolarmente sentita con riferimento al fenomeno del riciclaggio, che, come si è esaminato, il legislatore europeo ha giustamente previsto di sanzionare penalmente, ma, nel tentativo di raggiungere la completezza, nell'ampio catalogo di condotte da punire ne ha previste molte che non sono neppure riferite a comportamenti idonei a mascherare l'origine illegale dei proventi, quali il possesso e l'utilizzo di beni di provenienza illecita. Questo notevole ampliamento delle condotte da sanzionare a titolo di riciclaggio, oltre ad aver creato difficoltà in sede di attuazione, pone anche problemi di compatibilità col principio della libertà d'iniziativa economica. Per altro verso, nonostante la volontà di compiutezza, la direttiva 2018/1673/UE sulla lotta al riciclaggio mediante il diritto penale ha completamente ignorato il fenomeno diffuso e tutt'altro che innocuo dei *financial manager* o *money mule*, che con la loro opera consentono di nascondere la derivazione illecita dei proventi dei crimini informatici. Il risultato è che in nessuno dei tre ordinamenti esaminati è stata chiaramente inquadrata la responsabilità penale del *financial manager*, che può, a seconda dei casi, essere ritenuto responsabile a titolo di concorso nel

reato di frode informatica o di riciclaggio. Si ritiene, dunque, che il legislatore europeo potrebbe intervenire anche per regolare la responsabilità penale di tali soggetti.

È giusto e doveroso che il legislatore europeo intervenga in materie che presentano indubbi profili transnazionali, qual è senz'altro il *cybercrime*, ma il suo intervento non può limitarsi a riprendere il contenuto di vecchie decisioni quadro, con l'aggiunta di ulteriori singole condotte da sanzionare del tutto simili a quelle già previste per singoli oggetti di reato, perché questo reca solo confusione nei legislatori degli Stati membri che, presentando già all'interno dei loro codici penali diverse fattispecie per sanzionare i reati informatici e cibernetici, non riescono a comprendere la portata della direttiva e a tradurla in una normativa nazionale efficace. Non per nulla, infatti, nei provvedimenti di attuazione dei tre ordinamenti presi in considerazione nel presente lavoro viene sempre più spesso specificato che la normativa nazionale viene ritenuta in larga parte già conforme alla direttiva. Nella maggior parte dei casi, pertanto, le modifiche sono assolutamente superflue e di facciata, se non addirittura dannose, come nei casi in cui il legislatore si è limitato a riprodurre gran parte del testo della direttiva, creando nuove fattispecie quasi identiche ad altre già esistenti, unicamente per evitare una procedura d'infrazione o per chiuderne una già avviata.

La mancata piena armonizzazione auspicata, infatti, è frutto anche di questa tecnica legislativa, che non tiene in considerazione il fatto che ormai in tutti gli ordinamenti europei sono già presenti reati informatici. Come si è avuto modo di esaminare, a seguito dell'attuazione della direttiva 2019/713/UE le legislazioni italiana, tedesca e spagnola in materia di frode e falsificazione degli strumenti di pagamento diversi dai contanti sono ancora più diverse tra loro di quanto lo fossero prima della sua adozione. Questo perché il legislatore europeo non ha chiarito, come invece avrebbe dovuto fare, la differenza tra la frode informatica, da un lato, e, dall'altro, la falsificazione e indebito utilizzo di strumenti di pagamento immateriali diversi dai contanti. Il paradosso è che i legislatori che hanno correttamente deciso di dare attuazione a tutti gli articoli della menzionata direttiva, ovvero quello italiano e spagnolo, si ritrovano oggi all'interno dei loro codici penali due fattispecie che hanno molti punti in comune e che nella maggior parte degli attacchi informatici possono trovare entrambe applicazione, dato che l'alterazione di uno strumento immateriale diverso dai contanti (quindi informatico), coincide con la condotta di alterazione/manipolazione di un sistema informatico, con conseguente ingiustificata duplicazione delle previsioni sanzionatorie.

È opportuno, quindi che il legislatore europeo intervenga quanto prima per correggere le storture del sistema. Inoltre, sarebbe opportuno che lo stesso promuovesse una

procedura coordinata tra Stati europei per l'attuazione delle direttive, in modo da evitare che poi ciascuno Stato adotti soluzioni completamente diverse da quelle degli altri, impedendo così che venga raggiunto l'obiettivo di armonizzazione auspicato. A tal fine, una soluzione di facile adozione e senza costi potrebbe essere quella di prevedere la condivisione dei diversi progetti di legge preparati dai singoli Stati membri con quella degli altri legislatori nazionali: un controllo e un confronto preventivo, prima dell'adozione degli atti normativi potrebbero evitare future incoerenze.

Infine, una considerazione va fatta anche per quanto riguarda la giurisdizione. Si auspica che il legislatore europeo quando prevede l'obbligo per gli Stati membri di adottare le misure necessarie a stabilire la propria giurisdizione per i reati cibernetici, abbandoni il criterio obsoleto della territorialità, che sul *web* è quasi inapplicabile, data la sua diffusione globale, e, invece, adotti quale criterio principale quello della personalità passiva e/o della collocazione dei server che hanno subìto l'attacco informatico. In questo modo gli Stati membri sarebbero costretti ad adeguare la loro normativa sul punto, con indubbi vantaggi dal punto di vista della tutela delle vittime.

Bibliografia

AA. VV., *Automatically Dismantling Online Dating Fraud*, in *IEEE Trans. Inf. Forensics Secur*., 2020, vo. 15, p. 1128 ss.

AA.VV., *Bitcoin - Asset or Currency? Revealing Users' Hidden Intentions*, in *European Conference on Information Systems - Tel Aviv*, 2014

AA.VV., *Cyber-OC-Scope and manifestation in selected EU member states*, Wiesbaden, 2016

AA. VV., *Detecting Ethereum Ponzi Schemes Based on Improved LightGBM Algorithm*, in *IEEE Trans. Inf. Forensics Secur*., 2022, vol. 9, n. 2, p. 624 ss.

AA. VV., *Exploring how, why and in what contexts older adults are at risk of financial cybercrime victimisation: A realist review*, in *Exp. Gerontol*., 2022, vol. 159, p.1 ss.

AA.VV., *Online Romance Scams: Relational Dynamics and Psychological Characteristics of the Victims and Scammers. A Scoping Review*, in *Clin. Pract. Epidemiol. Ment. Health*., 2020, n. 16, p. 24 ss.

AA.VV., *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*, 2018, *Report* disponibile *online* all'indirizzo https://arxiv.org/abs/1802.07228

AA. VV., *Ransomware: Recent advances, analysis, challenges and future research directions*, in *Comput. Secur*, 2021, vol. 111, p. 1 ss.

AA. VV., *Understanding the Dark Web*, in B. Akhgar, M. Gercke, S. Vrochidis, H. Gibson (eds.), *Dark Web Investigation*, 2021, Cham, p. 3 ss.

ABADÍAS SELMA A., FERNÁNDEZ ALBESA N., LEAL RUIZ R., *Ciberdelincuencia. Temas prácticos para su estudio*, A Coruña, 2021

ABEL SOUTO M., *El delito de blanqueo en el Código penal español. Bien juridico protegido, conductas típicas y objecto material tras la Ley orgánica 15/2003, de 25 de noviembre*, Barcelona, 2005

ABEL SOUTO M., *Expansión española del blanqueo de dinero en la última década de reformas penales*, in S. Cornejo Aguiar (dir.), I.P. Guevara Vásquez (dir.), G. E. Piva Torres (coord.), *Selecciones de dogmática penal latinoamericana. Presente y futuro*, Barcelona, 2020, p. 381 ss.

ABEL SOUTO M., *El nuevo tipo agravado de blanqueo en el ejercicio profesional de los obligados por la normativa de prevención*, in *Revista penal México*, 2022, n. 20, p. 17 ss.

ACCINNI G., *L'utilizzo criminogeno della* blockchain*: gli* smart contract, in *Sist. Pen*., 2022, n. 6, p. 133 ss.

ALBERS M., *Informationelle Selbstbestimmung*, Baden-Baden, 2005

ALBRECHT M., *Die Kriminalisierung von Dual-Use-Software*, Berlin, 2014

ALMOMANI A., GUPTA B.B., ATAWNEH A., MEULENBERG A. e ALMOMANI E., *A Survey of Phishing Email Filtering Techniques*, in *Comm. Surv. Tutor.*, 2013, Vol. 15, n. 4, p. 2070 ss.

ALONSO PÉREZ F., *Delitos Contra el Patrimonio y contra el orden socioeconómico. Aspectos penales y criminológicos*, Madrid, 2003

ALTENHAIN K., FLECKENSTEIN L., *Der Gesetzentwurf zur Neufassung des § 261 StGB*, in *JZ*, 2020, n. 21, p. 1045 ss.

AMATO G., *Il riciclaggio del denaro "sporco". La repressione penale dei profitti delle attività illecite*, Roma, 1993

AMBOS K., *Internationales Strafrecht*, München, 2018

AMBROSETTI E.M., *Problemi attuali in tema di reato continuato. Dalla novella del 1974 al nuovo codice di procedura penale*, Padova, 1991

AMOAH B., *Mr Ponzi with Fraud Scheme Is Knocking: Investors Who May Open*, in *Glob. Bus. Rev.*, 2018, vol. 19, n. 5, p. 1115 ss.

ANARTE BORRALLO E., *Incidencia de las nuevas tecnologías en el sistema penal. Aproximación al Derecho Penal en la sociedad de la información*, in *Derecho y conocimiento. Anuario jurídico sobre la sociedad de la información*, 2001, vol. 1, p. 191 ss.

ANGIONI F., *Contenuto e funzioni del concetto di bene giuridico*, Milano, 1983

ANTOLISEI F., *Manuale di diritto penale. Parte speciale*, vol. I, XVI ed. a cura di C.F. Grosso, Milano, 2016

ANTÓN ONECA J., voce *Estafa*, in C.E. Mascareñas (dir.), *Nueva Enciclopedia jurídica*, vol. XI, Barcelona, 1975, p. 57 ss.

ANGELOTTI D., *Delitti contro il patrimonio*, in E. Florian (a cura di), *Trattato di diritto penale*, 4° ed. agg., Milano, 1936

ARÁNGUEZ SÁNCHEZ C., *El Delito de Blanqueo de Capitales*, Madrid, 2000

ATERNO S., *La Cassazione non convince sull'intercettazione illecita di comunicazioni informatiche e telematiche*, in *Cass. pen.*, 2005, n. 5, p. 1582 ss.

ATERNO S., *Sull'accesso abusivo a un sistema informatico o telematico*, in *Cass. pen.*, 2000, n. 11, p. 2994 ss.

BACIGALUPO ZAPATER E., *Falsedad documental, estafa y administración desleal*, Madrid, 2007

BAJO FERNÁNDEZ M., BACIGALUPO SAGGESE S., *Derecho penal económico*, Madrid, 2010

BAJO FERNÁNDEZ M., BACIGALUPO SAGGESE S. (dir.), *Política Criminal y blanqueo de capitales*, Madrid, 2009

BARILE L., *Appropriazione indebita di file informatici: tra interpretazione estensiva e divieto di analogia il diritto penale è 'cosa mobile'*, in *Sist. pen.*, 2021, n. 3, p. 139 ss.

BARTOLETTI M., CARTA S., CIMOLI T., SAIA R., *Dissecting Ponzi schemes on Ethereum: identification, analysis, and impact*, in *Future Gener. Comput. Syst*., 2020, Vol. 102, p. 259 ss.

BARTOLI R., *La frode informatica tra "modellistica", diritto vigente, diritto vivente e prospettive di riforma*, in *Dir. informatica*, 2011, n. 3, p. 383 ss.

BARTON S., *Sozial übliche Geschäftstätigkeit und Geldwäsche (§ 261 StGB)*, in *StV*, 1993, n. 3, p. 156 ss.

BASILE E., *L'autoriciclaggio nel sistema penalistico di contrasto al* money laundering *e il nodo gordiano del concorso di persone*, in *Cass. pen*., 2017, n. 3, p. 1277 ss.

BAUR D.G., HONG K., LEE A.D., *Bitcoin: Medium of exchange or speculative assets?*, in *J. Int. Financial Mark. Inst. Money*, 2018, vol. 54, p. 177 ss.

BAVETTA G., voce *Identità (diritto alla)*, in *Enc. dir*., vol. XIX, Milano, 1970, p. 953 ss.

BECK S., BUCHARD C., FATEH-MOGHADAM B. (Hrsg.), *Strafrechtsvergleichung als Problem un Lösung*, Baden-Baden, 2011

BELE J., *Cryptocurrencies as facilitators of cybercrime*, in *SHS Web Conf*., 2021, vol. 111, p. 1 ss.

BELLACOSA M., *Il luogo di consumazione del delitto di accesso abusivo a un sistema informatico o telematico: in attesa delle Sezioni Unite*, in *Dir. Pen. Cont*., 2 febbraio 2015, p. 1 ss.

BELTRANI S., *Reati informatici e d.lgs. 231/2001 alla luce della legge di attuazione della Convenzione di Budapest*, in *Resp. amm. società e degli enti*, 2008, n. 4, p. 21 ss.

BERGHELLA F., BLAIOTTA R., *Diritto penale dell'informatica e beni giuridici*, in *Cass. pen*., 1995, n. 9, p. 2329 ss.

BERNARDONI P., *Attuazione degli obblighi europei in materia di lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti: prima lettura del d.lgs. n. 184 del 2021*, in *Sist. pen*., 3 febbraio 2021

BETTIOL G., *Concetto penalistico di patrimonio e momento consumativo della truffa*, in *Giur. it.*, 1947, parte IV, oggi anche in Id., Scritti giuridici, vol. II, Padova, 1966, p. 713 ss.

BINDING K., *Lehrbuch des Gemeinen Deutschen Strafrechts. Besonderer Teil*, Leipzig, 1902

BLANCO CORDERO I., *El Delito de Blanqueo de Capitales*, Cizur Menor, 2015

BOCCHINI R., *Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche*, in *Dir. inf. inf.*, 2017, n. 1, p. 27 ss.

BODDY M., *Phishing 2.0: the new evolution in cybercrime*, in *Comput. Fraud Secur.*, 2018, n. 11, p. 8 ss.

BONAIUTI G., *Schemi di pagamento e valute virtuali*, in *Moneta e Credito*, 2019, vol. 72, n. 288, p. 389 ss.

BORDY R., KERN S., OGUNADE K., *An insider's look at the rise of Nigerian 419 scams*, in *J. Financ. Crime*, 2022, vol. 29, n. 1, p. 202 ss.

BORGES G., SCHWENK J., STUCKENBERG C., WEGENER C., *Identitätsdiebstahl und Identitätsmissbrauch im Internet. Rechtlische und technische Aspekte*, Heidelberg, 2011

BOSCH S., *Straftaten in virtuellen Welten. Eine materiellrechtliche Untersuschung*, Berlin, 2018

BOYCE B., *Cyber Extortion – The Corporate Response*, in *Comput. Secur*., 1997, n. 16, p. 25 ss.

BRANDS J., DOORN J.V., *The Measurement, Intensity and Determinants of Fear of Cybercrime: A systematic review*, in *Comput. Hum. Behav.*, 2022, vol. 127, p. 1 ss.

BRICCHETTI R., *Riciclaggio e auto-riciclaggio*, in *Riv. it. dir. proc. pen*., 2014, n. 2, p. 684 ss.

BRICOLA F., *Teoria generale del reato*, estr. da *Noviss. Dig. it.*, vol. XIX, Torino, 1973 oggi anche in Id., *Scritti di diritto penale*, vol. I, a cura di S. Canestrari e A. Melchionda, Milano, 1997, 542 ss.

BRIZZI F., *I profili penali del ransomware*, in *Il processo telematico*, 21 febbraio 2002, p. 7, disponibile *online* all'indirizzo ilprocessotelematico.it

BRODOWSKI D., *Stellungnahme zum Gesetzentwurf der Bundesregierung: Entwurf eines Gesetzes zur Änderung des Strafgesetzbuches – Strafbarkeit des Betreibens krimineller Handelsplattformen im Internet und des Bereitstellens entsprechender Server-Infrastrukturen (BT-Drs. 19/28175)*, 2021, p. 1 ss., disponibile *online* all'indirizzo https://kripoz.de/wp-content/uploads/2021/05/stellungnahme-brodowski-betreiben-kriminaller-handelsplattformen.pdf

BRZESZCZYŃSKI, J., GAJDKA J., SCHABEK T., *Bitcoin as a New Currency*, in *Folia Oecon.*, 2020, vol. 20, n. 2, p.49 ss.

BUSCH R., *Die systematische Behandlung der sog. Vermögensdelikte im kommenden Strafrecht*, in *Zstw*, 1937, vol. 56, p. 676 ss.

BUSSMAN K.D., *Geldwäscheprävention im Markt - Funktionen, Chancen und Defizite*, 2018, Berlin

BUSSOLATI N., *Accesso abusivo a un sistema informatico o telematico ex art. 615-ter c.p.: il nodo* dell'abusività, in *Stud. Iuris*, 2018, n. 4, p. 428 ss.

BÜLTE J., *Stellungnahme zum Entwurf eines Gesetzes zur Verbesserung der strafrechtlichen Bekämpfung der Geldwäsche, Ausschuss für Recht und Verbraucherschutz des Deutschen Bundestages am 9. Dezember 2020*, disponibile *online* al sito https://www.bundestag.de/resource/blob/810652/881114134916dc4b59a8cdeacb511623/buelte_neu-data.pdf

CABEDO VILLAMÓN F., ORTIZ NAVARRO J.F., AGUADO LÓPEZ S., *Conductas típicas y prueba electrónica en los fraudes electrónicos*, in C. Sanchis Crespo, *Fraude*

electrónico. Panorámica actual y medios jurídicos para combatirlo, Cizur Menor, 2013, p. 241 ss.

CADOPPI A., CANESTRARI S., MANNA A., PAPA M. (a cura di), *Cybercrime*, Torino, 2019

CADOPPI A., CANESTRARI S., MANNA A., PAPA M. (a cura di), *Trattato di diritto penale. Parte generale e speciale. Riforme 2008-2015*, Torino, 2015, p. 921 ss.

CADWELL M., ANDREWS J.T.A., TANAY T., GRIFFIN L.D., *AI-enabled future crime*, in *Crime Sci.*, 2020, vol. 9, n. 14, p. 1 ss.

CAJANI F., *Profili penali del phishing*, in *Cass. pen.*, 2007, n. 6, p. 2294 ss.

CAJANI F., COSTABILE G., MAZZARACO G., *Phishing e furto d'identità digitale. Indagini informatiche e sicurezza bancaria*, Milano, 2008

CAJANI F., *La tutela penale dell'identità digitale alla luce delle novità introdotte dal d.l. 14 agosto 2013, n. 93 (convertito con modificazioni dalla l. 15 ottobre 2013, n. 119)*, in *Cass. pen.*, n. 3, 2014, p. 1094 ss.

CAJANI F., CAVALLO F., *Le truffe su piattaforma di e-commerce: l'esperienza della procura di Milano*, in G. Costabile, A. Attanasio, M. Ianulardo (a cura di), *IISFA Memberbook 2015 – Digital Forensic*, Forlì, 2015, p. 19 ss.

CALDERÓN CEREZO A., CHOCLÁN MONTALVO J.A., *Manual de Derecho Penal. Tomo II Parte Especial*, Barcelona, 2005

CALDERONI F., *The European legal framework on cybercrime: striving for an effective implementation*, in *Crime Law Soc Change*, 2010, vol. 54, p. 339 ss.

CALONI A., *Bitcoin: profili civilistici e tutela dell'investitore*, in *Riv. dir. civ.*, 2019, n. 1, p. 159 ss.

CAMPLANI F., Locus commissi delicti, *norme di collegamento e reati informatici a soggetto passivo indeterminato*, in *Arch. pen.*, 2020, n. 2, p. 1 ss.

CANCIO MELIÁ M., *Conducta de la víctimae imputación objectiva en Derecho Penal. Estudio sobre los ámbitos de responsabilidad de víctima y autor en actividades arriesgadas*, Barcelona, 1998

CAPACCIOLI S., *Criptovalute e bitcoin: un'analisi giuridica*, Milano, 2015

CAPACCIOLI S. (a cura di), *Criptoattività, criptovalute e bitcoin*, Milano, 2021

CARMONA A., *Tutela penale del patrimonio individuale e collettivo*, Bologna, 1996

CARPIO DELGADO J., *El delito de blanqueo de bienes en el nuevo Código penal*, Valencia, 1997

CASSANO G., *Contenuto e limiti del diritto all'identità personale (in margine allo sceneggiato sul caso "Re C*ecconi"), in *Dir. inf. inf.*, n.1, 1997, p. 118 ss.

CASTAGNO J.P., STIGLIANO A.A., *La tutela penale del patrimonio informativo aziendale tra appropriazione indebita di files e "presa di conoscenza" di informazioni*, in *Dir. di Internet*, 2020, n. 3, p. 489 ss.

CASTELLÓ NICÁS N., *El concurso de normas penales*, Granada, 2000

CASTIÑERA PALOU M., *El delito continuado*, Barcelona, 1977

CAVALLINI S, TROYER L., *Apocalittici o integrati? Il nuovo reato di autoriciclaggio: ragionevoli sentieri ermeneutici all'ombra del "vicino ingombrante"*, in *Riv. trim. dir. pen. cont*., 2015, n. 1, p. 95 ss.

CHANDRA Y., *Non-fungible token-enabled entrepreneurship: a conceptual framework*, in *J. Bus. Ventur. Insights*, 2022, n. 18, p. 1 ss.

CHOCLÁN MONTALVO J.A., *Estafa por computación y criminalidad económica vinculada a la informática*, in *Actualidad penal*, 1997, n. 47, p. 1068 ss.

CHOCLÁN MONTALVO J.A., *El delito continuado*, Madrid, 1997

CHOCLÁN MONTALVO J.A., *El delito de estafa*, Barcelona, 2000

CHOO K.R., *Cryptocurrency and Virtual currency: Corruption and Money Laundering/Terrorism Financing Risks?*, in D.L. Kuo Chuen, *Handbook of digital currency. Bitcoin, innovation, financial instruments, and big data*, Amsterdam, 2015, p. 283 ss.

CIAN M., *La criptovaluta. Alle radici dell'idea giuridica di denaro attraverso la tecnologia: spunti preliminari*, in *Banca borsa*, 2019, n. 3, p. 315 ss.

CIPOLLA P., *Social network, furto di identità e reati contro il patrimonio*, in *Giur. merito*, 2012, n. 12, p. 2672 ss.

CIPOLLA P., *E-commerce e truffa*, in *Giur. mer*., 2013, n. 12, p. 2624 ss.

CIVELLO CONIGLIARO S., *La nuova tutela penale europea dei sistemi di informazione. Una prima lettura della direttiva 2013/40/UE del Parlamento europeo e del Consiglio*, in *Dir. pen. cont.*, 30 ottobre 2013, p. 1 ss.

CLOUGH J., *Principles of Cybercrime*, Cambridge, 2015

COCUCCIO M.F., *Il diritto all'identità personale e l'identità "digitale",* in *Dir. fam. e pers.*, n. 3, 2016, p. 949 ss.

COLÁS TURÉGANO A., *Nuevas conductas delictivas contra la intimidad (arts. 197; 197 bis; 197 ter)*, in J.L. González Cussac (dir.) e Á. Matallín Evangelio, E. Górriz Royo (coord.), *Comentarios a la Reforma del Código Penal de 2015*, Valencia, 2015, p. 663 ss.

CONNOLLY A. Y., BORRION H., *Reducing Ransomware Crime: Analysis of Victims' Payment Decisions*, in *Comput. Secur*., 2022, vol. 119, p. 1 ss.

CONTI L., voce *Estorsione*, in *Enc. Dir*., vol. XV, Milano, 1966, p. 995 ss.

CORBET S., LUCEY B., URQUHART A., YAROVAYA L., *Cryptocurrencies as a financial asset: A systematic analysis*, in *Int. Rev. Financial Anal.*, 2019, vol. 62, p. 182 ss.

CORCOY BIDASOLO M., MIR PUIG S. (dir.), *Comentario al Código Penal. Reforma LO 5/2010*, Valencia, 2011

CORNELIUS K., *Sub 102 Besonderer Teil des Strafgesetzbuches*, in J. Taeger, J. Pohle (Hrsg.), *Computerrechts-Handbuch. Informationstechnologie in der Rechts-und Wirtschaftpraxis*, München, 2021, disponibile *online* al sito https://beck-online.beck.de

CORRADINO M., *La tutela penale del sistema dei pagamenti nell'abuso di carta di credito*, in *Banca, borsa, tit. cred.*, 2001, n. 1, p. 121 ss.

CORRIAS LUCENTE G., *Brevi note in tema di accesso abusivo e frode informatica: uno strumento per la tutela penale dei servizi*, in *Dir. Inf. Inf*., 2001, n. 3, p. 492 ss.

CRAMER P., *Vermögensbegriff und Vermögensschaden im Strafrecht*, Bad Homburg, 1968

CRISTANI A., voce *Falsità personale*, in *Dig. disc. pen.*, vol. V, Torino, 1991, p. 107 ss.

CROCE M., *Cyberlaundering e valute virtuali. La lotta al riciclaggio nell`era della distributed economy*, in *Sist. Pen.*, 2021, n. 4, p. 127 ss.

CROSS C., *No laughing matter: blaming the victim of online fraud*, in *Int. Rev. vict*., 2015, vol. 21, n. 2, p. 187 ss.

CROSS C., KELLY M., *The problem of "white noise": examining current prevention approaches to online fraud*, in *J. Financ. Crime*, 2016, vol. 23, n. 4, p. 806 ss.

CRUZ DE PABLO J.A., *Derecho penal y nuevas tecnologías. Aspectos sustantivos. Adaptado a la reforma operada en el Código Penal por Ley Orgánica 15/2003 de 25 noviembre, especial referencia al nuevo artículo 286 CP*, Madrid, 2006

CUOMO L., *La tutela penale del domicilio informatico*, in *Cass. pen*., 2000, n. 11, p. 2990 ss.

DAI C., MASUDA K., KISHIMOTO Y. (eds.), *Blockchain and cryptocurrency. Building a High Quality Marketplace for Crypto Data*, Singapore, 2020

D'AIETTI G., *La tutela dei programmi e dei sistemi informatici*, in R. Borruso, G. Buonomo, G. Corasaniti, G. D'Aietti (a cura di), *Profili penali dell'informatica*, Milano, 1994, p. 39 ss.

DASKALAKIS N., GEORGITSEAS P., *An introduction to Cryptocurrencies. The Crypto Market Ecosystem*, London, 2020

D'ARCANGELO F., *L'accesso abusivo ad un sistema informatico nell'era di Internet*, in *Corr. Merito*, 2008, n. 10, p. 1066 ss.

DEEM D., *Notes from the field: observations in working with the forgotten victims of personal financial crimes*, in *J. Elder Abuse Negl*., 2000, vol. 12, n. 2, p. 33 ss.

DE FLAMMINEIS S., *Art. 615-ter c.p.: accesso legittimo ma per finalità estranee ad un sistema informatico*, in *Cass. pen*., 2011, n. 6, p. 2209 ss.

DE FRANCESCO G., *Lex specialis. Specialità ed interferenza nel concorso di norme penali*, Milano, 1980

DE MARSICO A., *Delitti contro il patrimonio*, Napoli, 1951

DE LA MATA BARRANCO N.J., DOPICO GÓMEZ-ALLER J., LASCURAÍN SÁNCHEZ J.A., NIETO MARTÍN A., *Derecho penal económico y de la empresa*, Madrid, 2018

DEL CARPIO DELGADO J., *La posesión y utilización como nuevas conductas en el delito de blanqueo de capitales*, in *Revista General de Derecho Penal*, 2011, n. 15, p. 1 ss.

DELGADO-MOHATAR O., SIERRA-CÁMARA, ANGUIANO E., *Blockchain-based semi-autonomous ransomware*, in *Future Gener. Comput. Syst*., 2020, vol. 112, p. 589 ss.

DELL'OSSO A.M., *Il reato di autoriciclaggio: la politica criminale cede il passo a esigenze mediatiche e investigative*, in *Riv. it. dir. proc. pen*., 2015, n. 2, p. 796 ss.

DELL'OSSO A.M., *Riciclaggio Di Proventi Illeciti e Sistema Penale*, Torino, 2017

DELOGU T., *Il momento consumativo della truffa*, in *Giur. Cass. pen*., 1944, vol. XIV, p. 68 ss.

DELOGU T., *Contributo alla teoria dei reati accessori*, in *Giust. pen*., 1947, II, p. 321 ss.

DEL TUFO V., *Profili critici della vittimo-dommatica. Comportamento della vittima e delitto di truffa*, Napoli, 1990

DEL VALLE SIERRA LÓPEZ M., *Los delitos de descubrimiento y revelación de secretos en el Código Penal de 2015: artículos 197,197 bis,197 ter, 197 quáter, 197 quinquies y 198*, in J. Del Carpio Delgado (dir.), *Algunas Cuestiones de Parte Especial tras la Reforma de 2015 del Código Penal*, Valencia, 2018, p. 132 ss.

DE STASIO V., *Verso un concetto europeo di moneta legale: valute virtuali, monete complementari e regole di adempimento*, in *Banca borsa*, 2018, n. 6, p. 747 ss.

DESTITO V., DEZZANI G., SANTORIELLO C., *Il diritto penale delle nuove tecnologie*, Padova, 2007

DE URBANO CASTRILLO E., *Los delitos informáticos tras la reforma del CP de 2010*, in *Delincuencia Informática. Tiempos de Cautela y Amparo*, Cizur Menor, 2012

DE VRIES B., TIGCHELAAR J., VAN DER LINDEN T., *Describing Identity Fraud: Towards a Common Definition*, in *SCRIPTed*, 2008, vol. 5, n. 3, p. 482 ss.

DHYRBERG A.H., *Bitcoin, gold and the dollar. A GARCH volatility analysis*, in *Finance Research Letters*, 2016, vol. 16, p. 85 ss.

DÍAZ Y GARCÍA CONLLEDO M., *La autoría en Derecho penal*, Barcelona, 1991

DIBIAGIO T.M., *Money Laundering and Drug Trafficking: A Question of Understanding the Elements of the Crime and the Use of Circumstantial Evidence*, in *U. Rich. L. Rev.*, 1994, vol. 28, p. 255 ss.

DÍEZ RIPOLLÉS J.L., *El blanqueo de capitales procedentes del trafico de drogas. La recepción de la legislación internacional en el ordenamiento penal español*, in *Actualidad penal*, 1994, n. 32, p. 582 ss.

DÍEZ RIPOLLÉS J.L., *Los elementos subetivos del delito. Bases metodológicas*, Buenos Aires, 2007

DÍEZ RIPOLLÉS J.L., *La racionalidad de las leyes penales. Practica y teoría*, Madrid, 2013

DOMBRET B., *Zahlungssysteme im Internet. Marksituation und Perspektiven*, Norderstedt, 2008

DONINI M., *Il principio di offensività. Dalla penalistica italiana ai programmi europei*, in *Riv. trim. dir. pen. cont*., 2013, n. 4, p. 4 ss.

DUGGTE S., *Vorbereitung eines Computerbetruges. Auf dem Weg zu einem „grenzlosen" Strafrecht*, in B. Heinrich (Hrsg.), *Festschrift für Ulrich Weber zum 70. Geburtstag*, Bielefeld, 2004, p. 285 ss.

EBERS M., HEINZE C., KRÜGEL T., STEINRÖTTER B. (Hrsg.), *Künstliche Intelligenz und Robotik*, München, 2020

EL-GHAZI M., LAUSTETTER C., *Das Gesetz zur Verbesserung der strafrechtlichen Bekämpfung der Geldwäsche – Ein Überblick über die wichtigsten Änderungen beim Straftatbestand des § 261 StGB und bei der selbständigen Einziehung nach § 76 a Abs. 4 StGB*, in *NZWiSt*, 2021, p. 209 ss.

ELLMER M., *Betrug und Opfermitverantwortung*, Berlin, 1986

EISELE J., *Schriftliche Stellungnahme zur Sachverständigenanhörung im Ausschuss für Recht und Verbraucherschutz des Deutschen Bundestages (BT-Drs. 19/28175)*, 2021, p. 1 ss., p. 2, disponibile *online* all'indirizzo https://www.bundestag.de/resource/blob/838700/b7ac31fd95c417ab9f52266f5f06f50c/stellungnahme-eisele-data.pdf

EISELE J., *Strafrecht Besonderer Teil. Eigentumsdelikte und Vermögensdelikte*, VI ed., Stuttgart, 2021

ERB V., SCHÄFER J. (Hrsg.), *Münchener Kommentar zum Strafgesetzbuch*, VI ed. München, 2021

ERB V., SCHÄFER J. (Hrsg.), *Münchener Kommentar zum Strafgesetzbuch*, V ed. München, 2022

ERNST S., *Das neue Computerstrafrecht*, in *NJW*, n. 37, 2007, p. 2661 ss.

ESER A., *Comparative criminal law. Development. Aims*, *Methods*, München, 2017

FAIELLA S., *Riciclaggio e crimine organizzato transnazionale*, Milano, 2009

FARALDO CABANA P., *Aspectos básicos del delito de blanqueo de bienes en el Código penal del 1995*, in *Estudios penales y criminológicos*, 1998, vol. 31, p. 117 ss.

FARALDO CABANA P., *Las nuevas tecnologías en los delitos contra el patrimonio y el orden socioeconómico*, Valencia, 2009

FARALDO CABANA P., *Antes y después de la tipificación expresa del autoblanqueo de capitales*, in *Estudios Penales y Criminológicos*, 2014, n. 34, p. 41 ss.

FARRÉ TREPAT E., *La tentativa de delito. Doctrina y jurisprudencia*, Madrid, 2011

FERNÁNDEZ-SALINERO SAN MARTIN M.A., *Las Estafas Piramidales y Su Trascendencia Jurídico Penal*, Madrid, 2019

FERNÁNDEZ TERUELO J.G., *Derecho penal e internet. Especial consideracióm de los delitos que afectan a jóvenes y adolescentes*, Valladolid, 2011

FIANDACA G., MUSCO E., *Diritto penale. Parte speciale. i delitti contro il patrimonio*, vol. III, Bologna, 2015

FIEDLER R., *Zur Strafbarkeit der einverständlichen Fremdgefährdung: unter besonderer Berücksichtigung des viktimologischen Prinzips*, Frankfurt am Main, 1990

FILIPKOWSKY W., *Cyber Laundering: An Analysis of Typology and Techniques*, in *Int. J. Crim. Justice Sci*., 2008, vol. 1, n. 3, p. 15 ss.

FINOCCHIARO G (a cura di), *Diritto all'anonimato*, Padova, 2008

FINOCCHIARO G., *Identità personale su internet: il diritto alla contestualizzazione dell'informazione*, in *Dir. inf. inf.*, 2012, n. 3, p. 383 ss.

FINOCCHIARO G., *La protezione dei dati personali e la tutela dell'identità*, in G. Finocchiaro, F. Delfini (a cura di), *Diritto dell'informatica*, Torino, 2014, p. 151 ss.

FINOCCHIARO S., *Il buio oltre la specialità. Le Sezioni Unite sul concorso tra truffa aggravata e malversazione*, in *Dir. pen. cont.*, 2017, n. 5, p. 344 ss., p.

FLICK G.M., *La repressione del riciclaggio ed il controllo dell'intermediazione finanziaria. Problemi attuali e prospettive*, in *Riv. it. dir. proc. pen*., 1990, n. 4, p. 1255 ss.

FLICK C., *Falsa identità su internet e tutela penale della fede pubblica degli utenti e della persona*, in *Dir. inf. inf.*, 2008, n. 4-5, p. 526 ss.

FLOR R., *Phishing, identity theft e identity abuse. Le prospettive applicative del diritto penale vigente*, in *Riv. it. dir. proc. pen.*, 2007, n. 2-3, p. 899 ss**.**

FLOR R., *Permanenza non autorizzata in un sistema informatico o telematico, violazione del segreto d'ufficio e concorso nel reato da parte dell'extraneus*, in *Cass. pen*., 2009, n. 4, p. 1509 ss.

FLOR R., *Verso una rivalutazione dell'art. 615 ter c.p.? Il reato di accesso abusivo a sistemi informatici o telematici fra la tutela di tradizionali e di nuovi diritti fondamentali nell'era di Internet*, in *Riv. trim. dir. pen. cont*., 2012, n. 2, p. 126 ss.

FLOR R., *Phishing e profili penali dell'attività illecita di "intermediazione" del cd. financial manager*, in *Dir. pen. proc.*, n. 1, 2012, p. 55 ss.

FLOR R., *I limiti del principio di territorialità nel cyberspace. Rilievi critici alla luce del recente orientamento delle Sezioni Unite*, in *Dir. pen. proc*., 2015, n. 10, p. 1291 ss.

FLOR R., *La condotta del pubblico ufficiale fra violazione della* voluntas domini*, "abuso" dei profili autorizzativi e "sviamento di potere"*, in *Dir. pen. proc*., 2018, n. 4, p. 506 ss.

FLOR R., LUPARIA L., *Criminalità organizzata e criminalità informatica ("cyberorganized crime")*, in *Dir. Pen. Cont.*, 2019, p. 202 ss.

FLORES PRADA I., *Criminalidad informática. Aspectos sustantivos y procesales*, Valencia, 2012

FLOREZ MENDOZA M., *Respuesta penal al denominado robo de identidad en las conductas de phishing bancario*, in *EPC*, 2014, vol. 34, p. 301 ss.

FOFFANI L., *Verso un nuovo diritto penale societario: i punti critici della legge delega*, in *Cass. pen.*, 2001, n. 11, p. 3246 ss.

FOFFANI L., *Verso un'armonizzazione europea del diritto penale dell'economia: la genesi di nuovi beni giuridici economici di rango comunitario, il ravvicinamento dei precetti e delle sanzioni*, in G. Grasso, L. Picotti e R. Sicurella (a cura di), *L'evoluzione del diritto penale nei settori d'interesse europeo alla luce del Trattato di Lisbona*, Milano, 2011, p. 583 ss.

FOFFANI L., *Economia, sistema bancario e intervento penale*, in *Dir. pen. proc*., 2016, n. 8, p. 985 ss.

FRANOSCH R., *Das Darknet – ein rechtsfreier Raum? Überlegungen zur Notwendigkeit einer Digitalen Agenda für das Straf- und Strafprozessrecht*, in P.E. Sensburg (Hrsg.), *Sicherheit in einer digitalen Welt*, 2017, Baden-Baden, p. 23 ss.

FRIEDEWALD M., LAMLA J., ROßNAGEL A. (Hrsg.), *Informationelle Selbstbestimmung im digitalen Wandel*, Wiesbaden, 2017

FROMBERG M., HAFFKE L., ZIMMERMANN P., *Kryptowerte und Eine Analyse der 5. Geldwäscherichtlinie sowie des Gesetzesentwurfs der Bundesregierung*, in *BKR*, 2019, p. 377 ss.

FROSALI R.A., *Concorso di norme e concorso di reati*, Milano, 1971

FUMO M., *La condotta nei reati informatici*, in *Arch. Pen*., 2013, n. 3, p. 771 ss.

GALÁN MUÑOZ A., *El fraude y la estafa mediante sistemas informáticos. Análisis del artículo 248.2 c.p.*, Valencia, 2005

GALÁN MUÑOZ A., *Los ciberdelitos en el ordenamiento español*, Barcelona, 2019

GALDIERI P., *Teoria e pratica nell'interpretazione del reato informatico*, Milano, 1997

GALLAS W., *Der Betrug als Vermögensdelikt*, in P. Bockelmann, W. Gallas (Hrsg.), *Festschrift für Eberhard Schmidt zum 70. Geburtstag*, Göttingen, 1961, p. 401 ss.

GALLEGO SOLER J.I., *Fundamento y límites de los deberes de autoprotección de la víctima en la estafa*, in *ADPCP*, 2005, vol. 8, p. 529 ss.

GARCÍA ALBERO R., *"Non bis in Idem" material y concurso de leyes penales*, Barcelona, 1995

GASPARRI G., *Timidi tentativi giuridici di messa a fuoco dei Bitcoin: miraggio monetario crittoanarchico o soluzione tecnologica in cerca di un problema?*, in *Dir. inf. inf.*, 2015, n. 3, p. 415 ss.

GAYVORONSKAYA T., MEINEL C., *Blockchain. Hype or innovation*, Cham, 2021

GAZEAS N., *Das neue Geldwäsche-Strafrecht: Weitreichende Folgen für die Praxis*, in *NJW*, 2021, p. 1041 ss.

GERCHE M., *Internet-related Identity Theft*, pubblicato sul portale del Council of Europe, *Discussion Paper on Internet-related Identity Theft*, Strasburgo, 2007, disponibile *online* al sito www.coe.int/cybercrime

GERCHE M., BRUNST P.W., *Praxishandbuch Internetstrafrecht*, Stuttgart, 2009

GERCHE M., *Die Entwicklung des Internetstrafrechts 2020/2021*, in *ZUM*, 2021, p. 921 ss.

GERHOLD S.F., *Strafbarkeit des Betreibens krimineller Internethandelsplattformen*, in *ZRP*, 2021, p. 44 ss.

GHAZI-TEHRANI A., PONTELL H., *Phishing Evolves: Analyzing the Enduring Cybercrime*, in *Vict. Offenders*, 2021, vol. 16, n. 3, p. 316 ss.

GILLESPIE A.A., *The Electronic Spanish Prisoner: Romance Frauds on the Internet*, in *J. Crim. L.*, 2017, vol. 81, no. 3, p. 217 ss.

GIUDICI A., *Creazione di un falso profilo utente sulla rete e delitto di sostituzione di persona*, in *Dir. pen. cont*., 25 giugno 2013, disponibile *online* all'indirizzo www.penalecontemporaneo.it

GOEL S., HONG Y., *Cyber War Games: Strategic Jostling Among Traditional Adversaries*, in Aa. Vv. (eds.), *Cyber Warfare. Building the Scientific Foundation*, Cham, 2015, p. 1 ss.

GÓMEZ BENITEZ J.M., *Función y contenido del error en el tipo de estafa*, in ID, *Estudios Penales*, Madrid, 2001, p. 149 ss.

GONZÁLES RUS J.J., *Aproximación al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos*, in *RFDUCM*, n. speciale 12, 1982, p.107 ss.

GONZÁLEZ RUS J.J., *Los intereses económicos de los consumidores. Protección penal*, Madrid, 1986

GONZÁLEZ RUS J.J., *Los delitos contra el patrimonio*, in B. Del Rosal Blasco (dir.), *Estudios sobre el nuevo Código Penal de 1995*, Valencia, 1997

GONZÁLES RUS J.J., *Protección penal de sistemas, elementos, datos, documentos, programas informáticos*, in *RECPC*, 1999, n. 1, p. 1 ss.

GONZÁLEZ RUS J.J., *Daños a través de internet y denegación de servicios*, in Aa. Vv., *Homenaje al profesor Dr. Gonzalo Rodríguez Mourullo*, Navarra, 2005, p. 1469 ss.

GÓRRIZ ROYO E., *El concepto de autor en derecho penal*, Valencia, 2008

GREGORI I., *Delitti contro il patrimonio e patrimonio dello Stato*, in *Annali dir. proc. pen*., 1935, p. 1171 ss.

GREVE V., *Die Zukunft des Europäischen Strafrechts: Rechtsdogmatische Vorgaben*, in U. Sieber (Hrsg.), *Europäische Einigung und Europäisches Strafrecht*, Berlin, 1993, p. 107 ss.

GROPP W., SINN A., *Strafrecht Allgemeiner Teil*, V ed., Berlin, 2020

GRÖSELING N., HÖFINGER F.M., *Hacking und Computerspionage - Auswirkungen des 41. StrÄndG zur Bekämpfung der Computerkriminalität*, in *MMR*, 2007, p. 549 ss.

GRÖSELING N., HÖFINGER F.M., *Computersabotage und Vorfeldkriminalisierung. Auswirkungen des 41. StrÄndG zur Bekämpfung der Computerkriminalität*, in *MMR*, 2007, p. 626 ss.

GRZYWOTZ J., KÖHLER O.M., RÜCKERT C., *Cybercrime mit Bitcoins – Straftaten mit virtuellen Währungen, deren Verfolgung und Prävention*, in *StV*, 2016, n. 11, p. 753 ss.

GRZYWOTZ J., *Virtuelle Kryptowährungen und Geldwasche*, Berlin, 2019

GULLO A., *Realizzazione plurisoggettiva dell'autoriciclaggio: la Cassazione opta per la differenziazione dei titoli di reato*, in *Dir. Pen. Cont.*, 2018, n. 6, p. 262 ss.

GUTIÉRREZ FRANCÉS M.L., *Fraude informático y estafa*, Madrid, 1991

GUTIÉRREZ FRANCÉS M.L., *Delincuencia económica e informática en el nuevo Código Penal*, in *CDJ*, 1996, n. 11, p. 247 ss.

HAFT F., *Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität (2. WiKG). Teil 2: Computerdelikte*, in *NStZ*, 1987, p. 6 ss.

HAGEL K., *Raub und Erpressung nach englischem und deutschem Recht und aus rechtsvergleichender Sicht*, Berlin, 1979

HANSEN D., *Strafbarkeit des Phishing nach Internetbanking-Legitimationsdaten*, Hamburg, 2007

HAZLETT P. H., LUTHER W. J., *Is bitcoin money? And what that means*, in *Q. Rev. Econ. Finance*, 2020, vol. 77, p. 144 ss.

HERRERO HERRERO C., *Infracciones penales patrimoniales*, Madrid, 2000

HERRMANN C., *Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*, Frankfurt am Main, 2010

HERZOG F., *Bitcoins und Geldwäsche: Bestandsaufnahme strafrechtlicher Fallgestaltungen und regulatorischer Ansätze*, in *StV*, 2019, n. 6, p. 412 ss.

HILGENDORF E., *Zweckverfehlung und Vermögensschaden beim Betrug*, in *JuS*, 1994, p. 466 ss.

HILGENDORF E., KUSCHE C., VALERIUS B., *Computer- und Internetstrafrecht. Ein Grundriss*, Heidelberg, 2022

HIRSCH B., *Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*, in *NJW*, 2008, p. 822 ss.

HIRSCH H.J., *Untauglicher Versuch und Tatstrafrecht*, in *Festschrift für Claus Roxin zum 70. Geburtstag*, 2001, Berlin, p. 711 ss.

HIRSCHBERG R., *Der Vermögensbegriff im Strafrecht. Versuch eines Systems er Vermögensdelikte*, Berlin, 1934

HÖINIGHAUS N., *Der hypothetische Vergleich des §269 StGB unter Berücksichtigung der tatsächlichen und normativen Vergleichbarkeit von Schrifturkunde und moderner (Computer-) Datenurkunde*, Stuttgart, 2005

HÖNIG M., *ICO und Kryptowährungen. Neue digitale Formen der Kapitalbeschaffung*, Wiesbaden, 2020

HUTCHINGS A., *Hacking and fraud: Qualitative analysis of online offending and victimization*, in K. Jaishankar, K. Routledge (eds.), *Global Criminology: Crime and Victimization in the Globalized Era*, Cambridge, 2013, p. 93 ss.

INGRASSIA A., *Le (caleidoscopiche) ricadute penalistiche della procedura di* voluntary disclosure*: causa sopravvenuta di non punibilità, autodenuncia e condotta penalmente rilevante*, in *Riv. trim. dir. pen. cont.*, 2015, n. 2, p. 127 ss.

INSOLERA G., voce *Concorso di persone nel reato*, in *Dig. disc. pen.*, vol. II, Torino, 1988, p. 437 ss.

INSOLERA G., *Diritto penale e criminalità organizzata*, Bologna, 1996

JAHN M., *Strafrecht AT und BT: Versuchter Computerbetrug durch Phishing Zum unmittelbaren Ansetzen beim versuchten Computerbetrug*, in *JuS*, 2012, p. 1135 ss.

JAKOBS G., *Urkundenfälschung*, Köln, 2000

JIMÉNEZ GARCÍA F. (dir.), ROPERO CARRASCO J. (dir.), PASTOR PALOMAR A. (coord.), *Blanqueo de capitales y corrupción. Interacciones para su erradicación desde el derecho internacional y los sistemas nacionales*, Cizur Menor, 2017

JOECKS W., *Studienkommentar StGB*, München, 2012

JOVER R.P., *Security Analysis of SMS as a Second Factor of Authentication: the challenges of multifactor authentication based on SMS, including cellular security deficiencies, SS7 exploits, and SIM swapping*, in *ACM queue*, 2020, vo. 18, n. 4, p. 37 ss.

KENJI-KIPKER D., *Informationelle Freiheit und staatliche Sicherheit. Rechtliche Herausforderungen moderner Überwachungstechnologien*, Tübingen, 2016

KILIAN W., *Property Rights und Datenschutz*, in W.A. Kaal, M. Schmidt e A. Schwartze (Hrsg.), *Festschrit zu Ehren von Christian Kirchner*, Tübingen, 2014, p. 901 ss.

KINDHÄUSER U., NEUMANN U., PAEFFGEN U. (Hrsg.), *Strafgesetzbuch. III Band*, V ed., Baden-Baden, 2017

KINDHÄUSER U., *Abhandlungen zum Vermögensstrafrecht*, Baden-Baden, 2018

KIRK D., *Identifying Identity Theft*, in *J. Crim. Law*, 2014, vol. 78, n. 6, p. 448 ss.

KOCHHEIM D., *Cybercrime und Strafrecht der Informations- und Kommunikationstechnik*, München, 2018

KOOPS B.J., LEENES R., *Identity Theft, Identity Fraud and/or Identity-related Crime*, in *DuD*, 2006, vol. 30, n. 9, p. 553 ss.

KOPP C., LAYTON R., SILLITOE J., GONDAL I., *The Role of Love stories in Romance Scams: A Qualitative Analysis of Fraudulent Profiles*, in *Int. J. Cyber Criminol*., 2015, vol. 9, n. 2, p. 205 ss.

KREUZBERG B., *Täterschaft und Teilnahme als Handlungsunrechtstypen. Zugleich ein Beitrag zur allgemeinen Verhaltensnormlehre*, Berlin, 2019

KSHETRI N., JEFFREY V., *Ransomware as a Business (RaaB)*, in *IT Professional*, 2022, vol. 24, n. 2, p. 83 ss.

KUSCHE C., *Die Strafbarkeit des Betreibens krimineller Handelsplattformen im Internet nach künftigem Recht*, in *JZ*, 2021, n. 1, p. 27 ss.

KÜPER W., *Die Absatzhilfe des Hehlers zwischen Täterschaft und Beihilfe*, in *JZ*, 2015, vol. 21, p. 1032 ss.

LACHNER K., KÜHL K., *Strafgesetzbuch Kommentar*, XXIX ed., München, 2018

LAMPE E., *Eigentumsschutz im Künftigem Strafrecht*, in H. Müller-Dietz (Hrsg.), *Strafrechtdogmatik und Kriminalpolitik*, Köln, 1971, p. 59 ss.

LAMPE E., *Der neue Tatbestand der Geldwäsche (§ 261 StGB)*, in *JZ*, 1994, p. 123 ss.

LAMPE E., *Tätersysteme: Spuren und Strukturen*, in *ZStW*, 2007, Vol. 119, n. 3, p. 471 ss.

LA TORRE M., *Il nome: contrassegno dell'identità personale*, in *Giust. civ*., 2013, n. 9, p. 443 ss.

LAUDATI A., *Terrorismo internazionale, criminalità organizzata e Money Transfer*, in *Per aspera ad veritatem*, 2002, n. 24, p. 25 ss.

LAURENZO COPELLO P., *Dolo y conocimiento*, Valencia, 1999

LAZZARI C., *Riciclaggio di carte di credito e truffa: concorso di reati o concorso di norme?*, in *Cass. pen*., 2001, n. 9, p. 2463 ss.

LEE C.S., *Online Fraud Victimization in China: A Case Study of Baidu Tieba*, in *Vict. Offenders*, 2021, vol. 16, n. 3, p. 343 ss.

LEIP C., *Der Straftatbestand der Geldwäsche - Zur Auslegung des § 261 StGB*, 1999, Berlin

LEMME G., PELUSO S., *Criptomoneta e distacco dalla moneta legale: il caso* bitcoin, in *Riv. dir. banc*., 2016, n. 4, p. 381 ss.

LEPERA M., *Un caso di reato semplice scambiato per reato circostanziato: sull'improbabile configurabilità dell'aggravante della "minorata difesa" in relazione alle truffe on-line*, in *Cass. Pen.*, 2017, n. 2, p. 687 ss.

LEVI M., REUTER P., *Money Laundering*, in *Crime & Just*., 2006, n. 34, p. 289 ss.

LEWIS J., *Economic Impact of Cybercrime—No Slowing Down*, *Report* per Center for Strategic and International Studies e McAfee, 2018, disponibile *online* al sito

https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf

LI W., CHEN H., NUNAMAKER J., *Identifying and Profiling Key Sellers in Cyber Carding Community: AZSecure Text Mining System*, in *Manag. Inf. Syst*., 2016, vol. 33, n. 4, p. 1059 ss.

LICHTENTHÄLER S., *Besitzverbot und Eigentumsschutz*, Tübingen, 2020

LIGGETT O'MALLEY R., HOLT K., *Cyber Sextortion: An Exploratory Analysis of Different Perpetrators Engaging in a Similar Crime*, in *J. Interpers. Violence*, 2022, vol. 37, n. 1-2, p. 258 ss.

LONGOBARDO C., *Impiego di denaro, beni o utilità di provenienza illecita*, in S. Fiore (a cura di), *I reati contro il patrimonio*, Torino, 2010, p. 884 ss.

LUCARELLI U., *La truffa. Aspetti penali, civili e processuali*, Padova, 2002

MABUNDA S., *Cyber Extortion, Ransomware and the South African Cybercrimes and Cybersecurity Bill*, in *Statute Law Rev*., 2019, vol. 40, n. 2, p. 143 ss.

MAGGINI A., *La truffa*, Padova, 1988

MAITLAND IRWIN A.S., RAYMOND CHOO K., LIU L., *An analysis of money laundering and terrorism financing typologies*, in *Journal of Money Laundering Control*, 2012, vol. 15, n. 1, p. 85 ss.

MAIWALD M., *Der Zueignungsbegriff im System der Eigentumsdelikte*, Heidelberg, 1970

MALGIERI G., *La nuova fattispecie di "indebito utilizzo d'identità digitale": un problema interpretativo*, in *Dir. pen. cont.- Riv. trim.*, n. 2, 2015, p. 143 ss.

MALGIERI G., *Il furto di "identità digitale": una tutela "patrimoniale" della personalità*, in R. Flor, D. Falcinelli, S. Marcolini (a cura di), *La giustizia penale nella rete. Le nuove sfide della società dell'informazione nell'epoca di Internet*, Milano, 2015, p. 37 ss.

MANCUSO V., STRANG A., FUNKE G.J., FINOMORE V.S., *Human factors of cyber attacks: a framework for human-centered research*, in *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 2014, vol. 58 n. 1, p. 437 ss.

MANES V., *Il riciclaggio dei proventi illeciti: teoria e prassi dell'intervento penale*, in *Riv. trim. dir. pen. econ*., 2004, n. 1-2, p. 35 ss.

MANES V., *Il principio di offensività nel diritto penale. Canone di politica criminale, criterio ermeneutico, parametro di ragionevolezza*, Torino, 2005

MANKY D., *Cybercrime as a service: a very modern business*, in *Comput. Fraud secur*., 2013, n. 6, p. 9 ss.

MANTOVANI F., *Contributo allo studio della condotta nei delitti contro il patrimonio*, Milano, 1962

MANTOVANI F., *Il principio di offensività del reato nella Costituzione*, in *Scritti in onore di Costantino Mortati*, vol. IV, Milano, 1977, p. 447 ss.

MANTOVANI F., *Il problema della offensività del reato nelle prospettive di riforma del codice penale*, in G. Vassalli (a cura di), *Problemi generali di diritto penale. Contributo alla riforma*, Milano. 1982, p. 63 ss.

MANTOVANI F., *voce Patrimonio (delitti contro il)*, in *Enc. Giur. Treccani*, Roma, 1990, vol. XXV, p. 1 ss.

MANTOVANI M., *Brevi note a proposito della nuova legge sulla criminalità informatica*, in *Crit. dir.*, 1994, IV, p. 12 ss.

MANTOVANI F., *Diritto penale, Parte Speciale, I delitti contro la persona*, vol. I, VI ed., Padova, 2016

MANTOVANI F., *Diritto penale, Parte Generale*, XI ed., Padova, 2020

MARBERTH-KUBICKI A., *Computer- und Internetstrafrecht*, München, 2010

MARGIOCCO M., *Frode informatica*, in G. Finocchiaro, F. Delfini, *Diritto dell'informatica*, Milano, 2014, p. 1107 ss.

MARINI G., voce *Estorsione*, in *Dig. disc. pen.*, vol. IV, Torino, 1992, p. 377 ss.

MARTÍN SAGRADO O., *La determinación del bien jurídico protegido por el delito de blanqueo de capitales y el autoblanqueo. Un debate que no cesa*, in *Boletín del Ministerio de Justicia*, 2018, n. 2206, p. 1 ss.

MARTÍNEZ PEÁLEZ R., RICO NOVELLA F., *Application of Electronic Currency on the Online Payment System like PayPal*, in AA. VV. (eds), *Project E-Society: Building Bricks*, Boston, 2006, Vol. 226, p. 44 ss.

MARTOS NÚÑEZ J.A., *El perjuicio patrimonial en el delito de estafa*, Madrid, 1990

MASI D., *Le criptoattività: proposte di qualificazione giuridica e primi approcci regolatori*, in *Banca impresa soc.*, 2021, n.2, p. 241 ss.

MATA Y MARTIN R.M., *El delito de robo con fuerza en las cosas*, Valencia, 1995

MATA Y MARTÍN R.M., *Delincuencia informática y derecho penal*, Madrid, 2001

MATA Y MARTÍN R.M., *Estafa Convencional, Estafa Informática y Robo en el Ámbito de los Medios Electrónicos de Pago. El Uso Fraudulento de Tarjetas y otros Instrumentos de Pago*, Pamplona, 2007

MATT H., RENZIKOWSKI J. (Hrsg.), *Strafgesetzbuch*, II ed., München, 2020

MAUME P., MAUTE L., FROMBERGER M., *Rechtshandbuch Kryptowerte. Blockchain, Tokenisierung, Initial Coins Offering*, München, 2020

MAURACH R. et al., *Strafrecht Besonderer Teil. Teil I Persönlichkeits- und Vermögenswerte*, XI ed., Heidelberg, 2019

MAZZACUVA N., *Il disvalore di evento nell'illecito penale. L'illecito commissivo doloso e colposo*, Milano, 1983

MECENATE A., *Il deposito del prezzo in criptomonete presso il notaio*, in *Riv. notariato*, 2021, n. 2, p. 385 ss.

MELE S., *Il Perimetro di Sicurezza Nazionale Cibernetica*, in *Dir. di Internet*, 2020, n. 1, p. 15 ss.

MENGONI E., *Accesso autorizzato al sistema informatico o telematico e finalità illecite: nuovo round alla configurabilità del reato*, in *Cass. pen*., 2011, n. 6, p. 2200 ss.

MERCALDO F., NARDONE V., SANTONE A., VISAGGIO C.A., *Ransomware steals your phone. Formal methods rescue it*, in *36th IFIP WG 6.1 International Conference on Formal Techniques for Distributed Objects, Components, and Systems*, Heidelberg, 2016, p. 212 ss.

MILITELLO V., *La tutela penale dei nuovi strumenti di pagamento: il caso del «sistema eurochecque»*, in *Foro it*., 1992, vol. 115, p. 617 ss.

MILITELLO V., *voce Patrimonio (delitti contro il)*, in *Dig. disc. pen*., Torino, 1995, vol. IX, p. 278 ss.

MILONE S., *La tutela dell'identità digitale nella nuova circostanza aggravante del delitto di frode informatica*, in *Legislazione pen.*, 2014, p. 133 ss.

MIQUELON-WEISSMAN M., *The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process?*, in *J. Marshall J. Computer & Info. L*., 2005, vol. 23, n.2, p. 329 ss.

MIR PUIG S., *Derecho Penal. Parte General*, X ed., Barcelona, 2015

MIRÓ LLINARES F., *Cibercrímenes económicos y patrimoniales*, en I. Ortiz De Urbina Gimeno (dir.), *Memento práctico penal y económico de la empresa 2011-2012*, Madrid, 2011, p. 469 ss.

MIRÓ LLINARES F., *La respuesta penal al ciberfraude. Especial atención a la responsabilidad de los muleros del phishing*, in *RECPC*, 2013, n. 15-12, p. 12:1 ss.

MITSILEGAS V., VAVOULA N., *The evolving EU anti-money laundering regime: challenges for fundamental rights and the rule of law*, in *Maastricht J. Eur. & Comp. L*., 2016, vol. 23, n. 2, p. 261 ss.

MOCCIA S., *Impiego di capitali illeciti e riciclaggio: la risposta del sistema penale italiano*, in *Riv. it. dir. proc. pen*., 1995, n. 3, p. 728 ss.

MOCCIA S., *Tutela penale del patrimonio e principi costituzionali*, Milano, 1988

MOLLE G., *I contratti bancari*, vol. XXXV, Tomo I, in AA.VV., *Trattato di diritto civile e commerciale Cicu-Messineo*, Milano, 1981

MONTI A., *Per un'analisi critica della natura giuridica delle criptovalute*, in *Rag. prat*., 2018, n. 2, p. 361 ss.

MOORE T., HAN J., CLAYTON R., The Postmodern Ponzi Scheme: Empirical Analysis of High-Yield Investment Programs, in A.D. Keromytis (eds.), *Financial Cryptography and Data Security. FC 2012. Lecture Notes in Computer Science*, Heidelberg, 2012, p. 41 ss.

MORABITO M.A., *Lo schema di decreto legislativo per l'attuazione della direttiva UE 2018/1673 sulla lotta al riciclaggio mediante il diritto penale: analisi e considerazioni*, in *Giur. pen. web.*, 2021, n. 9, p. 1 ss.

MORGANTE G., *Il reato come elemento del reato. Analisi e classificazione del concetto di reato richiamato dalla fattispecie penale*, Torino, 2013

MORÓN LERMA E., *Internet y Derecho Penal: Hacking y otras Conductas Ilícitas en la Red*, Pamplona, 2002

MUCCIARELLI F., *Commento all'art. 4 della legge 23 dicembre 1993 n. 547 - Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica*, in *Leg. pen.*, 1996, n. 1-2, p. 99 ss.

MUCCIARELLI F., *Qualche nota sul delitto di autoriciclaggio*, in *Dir. pen. cont.*, 2015, n. 1, p. 108 ss.

MUÑOZ CONDE F., GARCÍA ARÁN M., *Derecho Penal. Parte General*, X ed., Valencia, 2019

MUÑOZ CONDE F., *Derecho Penal. Parte Especial*, XXIII ed., Valencia, 2022

MUSCO E., ARDITO F., *Diritto penale fallimentare*, Bologna, 2018

MÜHLBAUER T., *Ablisten und Verwenden von Geldautomatenkarten als Betrug und Computerbetrug*, in *NStZ*, 2003, p. 650 ss.

MÜLLER M., *Neufassung des Geldwäschetatbestands – Der "all-crimes-approach"*, in *NJW-Spezial*, 2021, p. 312 ss.

MÜLLER W., *Aktuelle Probleme des § 263a StGB*, Frankfurt am Main, 1999

NEREMBERG L., *Forgotten Victims of Financial Crime and Abuse: Facing the Challenge*, in J. *Elder Abuse Negl.*, 2000, vol. 12, n. 2, p. 49 ss.

NESTLER N., *Bank- und Kapitalmarktstrafrecht*, Heidelberg, 2016

NESTLER N., *Hacker-Tools im StGB*, in *JURA*, 2021, n. 6, p. 629 ss.

NESTLER N., *Strafanwendungsrechtliche Probleme des reformierten Geldwäschetatbestands (Teil 2)*, in *JA*, 2022, n. 7, p. 814 ss.

NEUHEUSER S., *Die Strafbarkeit des Bereithaltens und Weiterleitens des durch „Phishing" erlangten Geldes*, in *NStZ*, 2008, p. 492 ss.

NIETHAMMER E., *Lehrbuch des Besonderen Teils des Strafrechts*, Tübingen, 1950

NIETO MARTÍN A., *¿Americanización o europeización del derecho penal económico?*, in *Rev. pen.*, 2007, n. 19, p. 120 ss.

NIETO MARTÍN A., GARCÍA-MORENO B., *Criptomonedas y derecho penal: más allá del blanqueo de capitales*, in *RECPC*, 2021, n. 23-17, p. 1 ss.

NILSSON H.G., *The Council of Europe Laundering Convention: A Recent Example of a Developing International Criminal Law*, in *Crim. L. Forum*, 1991, vol. 2, n. 3, p. 419 ss.

NORRIS G., BROOKES A., DOWELL D., *The Psychology of Internet Fraud Victimisation: a Systematic Review*, in *J. Police Crim. Psychol.*, 2019, vol. 34, p. 231 ss.

NUVOLONE P., *Il possesso nel diritto penale*, Milano, 1942

NUVOLONE P., *voce Fallimento (reati)*, in *Enc. Dir.*, vol. XVI, Milano, 1967, p. 476 ss.

OMOTE K., YANO M., *Bitcoin and Blockchain Technology*, in C. Dai, K. Masuda, Y. Kishimoto (eds.), *Blockchain and cryptocurrency. Building a High Quality Marketplace for Crypto Data*, Singapore, 2020, p. 129 ss.

O'KANE P., SEZER S., CARLIN D., *Evolution of ransomware*, in *IET Netw.*, 2018, n. 7, p. 321 ss.

OTTO H., *Die Struktur des strafrechtlichen Vermögensschutzes*, Berlin, 1970

PAGALLO U., QUATTROCOLO S., *The impact of AI on criminal law, and its twofold procedures*, in W. Bartfield, U. Pagallo, *Research handbook on the law of artificial intelligence*, Cheltenham, 2018, p. 385 ss.

PAGLIARO A., *Il delitto di bancarotta*, Palermo, 1957

PAGLIARO A., voce *Concorso di norme penali*, in *Enc. Dir.*, vol. III, Milano, 1961, p. 545 ss.

PAGLIARO A., voce *Falsità personale*, in *Enc. dir.*, vol. XVI, Milano, 1967, p. 646 ss.

PAGLIARO A., *Tutela della vittima nel sistema penale delle garanzie*, in *Riv. it. dir. e proc. pen.*, 2010, n. 1, p. 41 ss.

PALMA HERRERA J.M., *Los delitos de blanqueo de capitales*, Madrid, 2000

PALOMBI E. (a cura di), *Il riciclaggio dei proventi illeciti. Tra politica criminale e diritto vigente*, Napoli, 1996

PARODI C., *Profili penali dei virus informatici*, in *Dir. pen. proc.*, 2000, n. 5, p. 632 ss.

PARODI C., *Commercio elettronico e tutela penale dei mezzi di pagamento*, in *Dir. pen. proc.*, 2001, n. 1, p. 103 ss.

PARODI C., CALICE A., *Responsabilità penali e Internet. Le ipotesi di responsabilità penale nell'uso dell'informatica e della telematica*, Milano, 2001

PARODI C., *Tecnologia blockchain, bitcoin e riciclaggio: il futuro è adesso*, in *il penalista*, 14 maggio 2018, disponibile *online* al sito ilpenalista.it

PARODI C., SELLAROLI V. (a cura di), *Diritto penale dell'informatica. Reati della rete e sulla rete*, Milano, 2020

PASS R., SEEMAN L., SHELAT A., *Analysis of the blockchain protocol in asynchronous networks*, in Coron J.S., Buus Nielsen J. (eds.), *Advances in Cryptology. EUROCRYPT 2017. 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Cham, 2017, p. 643 ss.

PASTOR MUÑOZ N., *La determinación del engaño típico en el delito de estafa*, Madrid, 2004

PATCHIN J.W., HINDUJA S., *Sextortion Among Adolescents: Results From a National Survey of U.S. Youth*, in *Sex. abuse*, 2020, vol. 32, n. 1, p. 30 ss.

PAZIENZA F., *In tema di criminalità informatica: l'art. 4 della legge 23 dicembre 1993*, n. 547, in *Riv. It. dir. proc. pen*., 1995, n. 3, p. 750 ss.

PECORELLA C., *Il diritto penale dell'informatica*, Padova, 2006

PECORELLA C., *L'attesa pronuncia delle Sezioni Unite sull'accesso abusivo a un sistema informatico: un passo avanti non risolutivo*, in Cass. pen., 2012, n. 11, p. 3692 ss.

PECORELLA C., *Truffe on-line: momento consumativo e competenza territoriale*, in *Riv. it. dir. proc. pen*., 2012, n. 1, p. 113 ss.

PECORELLA G., voce *Patrimonio (delitti contro il)*, in *Noviss. Dig. It.*, vol. XII, Torino, 1965, p. 628 ss.

PECORELLA G., *Circolazione del denaro e riciclaggio*, in *Riv. it. dir. proc. pen*., 1991, n. 4, p. 1221 ss.

PEDRAZZI C., *Il concorso di persone nel reato*, Palermo, 1952, ora anche in PEDRAZZI C., *Scritti di diritto penale*. *Vol. I scritti di parte generale*, Milano, 2003, p. 3 ss.

PEDRAZZI C., *Inganno ed errore nei delitti contro il patrimonio*, Milano, 1955

PEDRAZZI C., *Postilla circa la competenza per territorio in materia di truffa*, in *Riv. It. Dir. proc. pen*., 1958, ora anche in ID, *Scritti di diritto penale*. *Vol. II scritti di parte speciale*, Milano, 2003, p. 359 ss.

PEDRAZZI C., *La riforma dei reati contro il patrimonio e contro l'economia*, in Aa. Vv., *Verso un nuovo Codice Penale. Itinerari-Problemi-Prospettive*, Milano, 1993, p. 350 ss.

PEDRAZZI C., SGUBBI F., *Reati commessi dal fallito. Reati commessi da persone diverse dal fallito*, in F. Galgano (a cura di), *Commentario Scialoja-Branca. Legge fallimentare*, Bologna, 1995

PEÑARANDA RAMOS E., *La participación en el delito y el principio de accesoriedad*, Madrid, 1990

PERRI P., *Lo smishing e il vishing, ovvero quando l'unico limite all'utilizzo criminale delle nuove tecnologie è la fantasia*, in *Dir. Internet*, n. 3, 2008, p. 261 ss.

PESTELLI G., *Riflessioni critiche sulla riforma dei reati di ricettazione, riciclaggio, reimpiego e autoriciclaggio di cui al d.lgs. 8 novembre 2021, n. 195*, in *Sist. Pen*., 2021, n. 12, p. 49 ss.

PETROCELLI B., *L'appropriazione indebita*, Napoli, 1933

PICA G., *Diritto penale delle tecnologie informatiche*, Torino, 1999

PICOTTI L., *La rilevanza penale degli atti di "sabotaggio" ad impianti di elaborazione dati*, in *Dir. inf. inf*., 1986, n. 3, p. 969 ss.

PICOTTI L., *Studi di diritto penale dell'informatica*, Verona, 1992

PICOTTI L., *Il dolo specifico. Un'indagine sugli "elementi finalistici" delle fattispecie penali*, Milano, 1993

PICOTTI L. *voce Reati informatici*, in *Enc. giur. Treccani*, VIII agg., Roma, 1999, p. 1 ss.

PICOTTI L., *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in ID. (a cura di), *Il diritto penale dell'informatica nell'epoca di Internet*, Padova, 2004, p. 21 ss.

PICOTTI L., *Internet e diritto penale: il quadro attuale alla luce dell'armonizzazione internazionale*, in *Dir. dell'Internet*, 2005, n. 2, p. 189 ss.

PICOTTI L., *La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale*, in *Dir. pen. proc*., 2008, n. 6, p. 700 ss.

PICOTTI L., *Limiti garantistici delle incriminazioni penali e nuove competenze europee alla luce del Trattato di Lisbona*, in G. Grasso, L. Picotti, R. Sicurella (a cura di), *L'evoluzione del diritto penale nei settori d'interesse europeo alla luce del Trattato di Lisbona*, Milano, 2011, p. 207 ss.

PICOTTI L., *I diritti fondamentali nell'uso ed abuso dei social network. Aspetti penali*, in *Giur. Mer*., 2012, n. 12, p. 2522 ss.

PICOTTI L. (a cura di), *Tutela penale della persona e nuove tecnologie, Quaderni per la riforma del codice penale*, Padova, 2013

PICOTTI L., *Profili penali del cyberlaundering: le nuove tecniche di riciclaggio*, in *Riv. trim. dir. pen. econ*., 2018, n. 3- 4, p. 590 ss.

PICOTTI L., *Cybersecurity: quid novi?*, in *Dir. di Internet*, 2020, n. 1, p. 11 ss.

PICOTTI L., *«Nuovi» crimini cibernetici e possibile rilevanza penale dell'intelligenza artificiale.* (*Atti digitali del convegno gli Stati Generali del diritto di Internet*, Luiss, 16,17,18 dicembre 2021), in *Diritto di Internet*, 2022, supplemento al n. 1, p. 1 ss.

PIERGALLINI C., *Autoriciclaggio, concorso di persone e responsabilità dell'ente: un groviglio di problematica ricomposizione*, in *Discrimen*, 2015, p. 539 ss.

PIERGALLINI C., VIGANÒ F., VIZZARDI M., VERRI A. (a cura di), *I delitti contro la persona. Libertà personale, sessuale e morale, domicilio e segreti*, in *Trattato di diritto penale. Parte speciale*, Vol. X, diretto da G. Marinucci ed E. Dolcini, Padova, 2015

PING H., *New Trends in Money Laundering – From the Real Word to Cyberspace*, in *J. Money Laund. Control*., 2004, vol. 8, n. 1, p. 48 ss.

PIVA D., *Il volto oscuro dell'autoriciclaggio: la fine di privilegi o la violazione di princìpi?*, in *Resp. amm. soc. enti*, 2015, n. 3, p. 59 ss.

PLANTAMURA V., *La tutela penale delle comunicazioni informatiche e telematiche*, in *Dir. inf. inf.*, 2006, n. 6, p. 847 ss.

PLANTAMURA V., *Domicilio e diritto penale nella società post-industriale*, Pisa, 2017

PLASSARAS N. A., *Regulating Digital Currencies: Bringing Bitcoin within the Reach of IMF*, in *Chi. J. Int'l. L.*, 2013, vol. 14, no. 1, pp. 377 ss.

PORXAS N., CONEJERO M., *Tecnología blockchain: funcionamento, aplicaciones y retos jurídicos relacionados*, in *Act. jur. Uría Menéndez*, 2018, n. 48, p. 24 ss.

PRIETO DEL PINO A.M., GARCÍA MAGNA D.I., MARTÍN PARDO A., *La deconstrucción del concepto de blanqueo de capitales*, in *InDret*, 2010, n. 3, p. 1 ss.

PRIETO DEL PINO A.M. (dir.), *Lessons of Spanish Substantive Criminal Law*, vol. II, Cizur Menor, 2020

PRIETO DEL PINO A.M., *Criminal offences against property and against the social-economic order in Spain: a global overview and a detailed approach to some particularly relevant issues*, in *Philia journal of Judicial Studies*, 2022, vol. 1, p. 82 ss.

PROSDOCIMI S., *Reato complesso*, in *Dig. pen.*, vol. XI, Torino, 1996, p. 213 ss.

PUPPE I., *Was ist Gesetzeskonkurrenz?*, in *JuS*, 2016, p. 961 ss.

QUEDENFELD R., *Handbuch Bekämpfung der Geldwäsche und Wirtschaftskriminalität*, 2017, Berlin

QUINTERO OLIVARES G., *Delitos contra el patrimonio y contra el orden socioeconómico*, in G. Quintero Olivares (dir.), J.M. Valle Muñiz (coord.), *Comentarios a la Parte Especial del Derecho Penal*, Pamplona, 1996, p. 441 ss.

QUINTERO OLIVARES G. (dir.), *Comentario a la reforma penal del 2015*, Cizur Menor, 2015

QUINTERO OLIVARES G., *De la extorsión*, in G. Quintero Olivares (dir.), Morales Prats F. (coord.), *Comentarios al Código Penal Español*, vol. II, VII ed., Cizur Menor, 2016, p. 69 ss.

RAGNO G., *Contributo alla configurazione del delitto di truffa processuale*, Milano, 1966

RAMESH BABU P., LALITHA BHASKARI D., SATYANARAYANA CH., *A Comprehensive Analysis of Spoofing*, in *JACSA*, 2010, vol. 1, n. 6, p. 157 ss.

RASCHKE A., *Geldwäsche und rechtswidrige Vortat – Eine Analyse der Irrtumsproblematik am Beispiel der Geldwäsche*, 2014, Baden-Baden

REGE A., *What's Love Got to Do with It? Exploring Online Dating Scams and Identity Fraud*, in *Int. J. Cyber Criminol*., 2009, vol. 3, n. 2, p. 494 ss.

RESTA G., *Identità personale e identità digitale*, in *Dir. inf. inf.*, 2007, n. 3, p. 511 ss.

RHEINECK B., *Zueignungsdelikte und Eigentümertineresse*, Berlin, 1979

RIBIC P., *The Nigerian email scam novel*, in *J. Postcolon. Writ.*, 2020, vol. 55, n. 3, p. 424 ss.

RICH T., *You can trust me: a multimethod analysis of the Nigerian email scam*, in *Secur J*, 2018, n. 31, p. 208 ss.

ROBLEDO VILLAR A., *Delitos contra el Patrimonio y el Orden socioeconómico. Comentarios a los articulos 234 a 289 del nuevo Código Penal*, Barcelona, 1997

ROCCO A., *L'oggetto del reato e della tutela giuridica penale. Contributo alle teorie generali del reato e della pena*, Torino, 1913, rist. Roma 1932

RODOTÁ S., *Il terribile diritto. Studi sulla proprietà privata*, Bologna, 1981

RODRIGUEZ MESA M.J., *Los delitos de daños. Capítulo IX del Título XIII del CP tras la reforma de la LO 1/2015*, Valencia, 2017

RODRIGUEZ MOURULLO G. (ed.), JORGE BARREIRO A. (coord.), *Comentarios al código penal*, Madrid, 1997

ROMANO M., *"Meritevolezza di pena", "bisogno di pena" e teoria del reato*, in *Riv. it. dir. proc. pen*., 1992, n. 1, p. 39 ss.

ROMEO CASABONA C.M., *Poder informático y seguridad jurídica*, Madrid, 1987

ROMEO CASABONA C.M., *Los delitos de descubrimiento y revelación de secretos*, Valencia, 2004

ROMEO CASABONA C.M., *La penetración del derecho penal económico en el marco jurídico europeo*, in C. M. Romeo Casabona, F. Flores Mendoza (dir.), *Nuevos instrumentos jurídicos en la lucha contra la delincuencia económica y tecnológica*, Granada, 2012, p. 331 ss.

ROMERO BARRANQUERO G., *Los elementos del tipo de estafa*, Buenos Aires, 1985

ROXIN C., *Strafrecht Allgemeiner Teil*, vol. II, München, 2003

ROXIN C., *Täterschaft und Tatherrschaft*, X ed., Berlin, 2019

ROXIN C., GRECO L., *Strafrecht Allgemeiner Teil*, vol. I, V ed., München, 2020

ROSEMBERGER P., *Bitcoin und Blockchain. Vom Scheitern einer Ideologie und dem Erfolg einer revolutionären Technik*, Berlin, 2018

ROVIRA DEL CANTO E., *Delincuencia informática y fraudes informáticos*, Granada, 2002

RUEDA MARTÍN A.M., *La confidencialidad, integridad y disponibilidad de los sistemas de información como bien jurídico protegido en los delitos contra los sistemas de información en el código penal español*, in *Riv. trim. Dir. pen. cont*., 2020, n. 3, p. 199 ss.

RUIZ VADILLO E., *Tratamiento de la delincuencia informática como una de las expresiones de la criminalidad económica*, in *PJ*, num. speciale IX, 1989, p. 53 ss.

RUTGER LEUKFELDT E., LAVORGNA A., KLEEMANS E.R., *Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime*, in *Eur J Crim Policy Res*., 2016, vol. 23, n. 3, p. 287 ss.

RUTHERFORD R., *The changing face of phishing*, in *Comput. Fraud secur.*, 2018, n. 11, p. 6 ss.

RYAN M., *Ransomware Revolution: The Rise of a Prodigious Cyber Threat*, Cham, 2021

SACHS M., KRINGS T., *Das neue „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme"*, in JuS, 2008, p. 481 ss.

SAHINGOZ O. K., BUBER E., ONDER D., BANU D., *Machine learning based phishing detection from URLs*, in *Expert Syst. Appl.*, 2019, Vol. 117, n. 3, p. 345 ss.

SAFFERLING C.J.M., *Die Abgrenzung zwischen strafloser Vorbereitung und strafbarem Versuch im deutschen, europäischen und im Völkerstrafrecht*, in *ZStW*, 2006, Vol. 118, n. 3, p. 682 ss.

SALVADORI I., *Los nuevos delitos informáticos en el Código penal español con la Ley Orgánica 5/2010. Perspectiva de derecho comparado*, in *ADPCP*, 2011, vol. 64, p. 221 ss.

SALVADORI I., *Il "microsistema" normativo concernente i danneggiamenti informatici. Un bilancio molto poco esaltante*, in *Riv. it. dir. e proc. pen.*, 2012, n. 1, p. 204 ss.

SALVADORI I., *Quando un* insider *accede abusivamente ad un sistema informatico o telematico? Le Sezioni Unite precisano l'ambito di applicazione dell'art. 615-ter c.p.*, in *Riv. Trim. Dir. Pen. Econ.*, 2012, n. 1-2, p. 369 ss.

SALVADORI I., *I reati di possesso. Un'indagine dogmatica e politico-criminale in una prospettiva storica e comparata*, Napoli, 2016

SALVADORI I., *Criminalità informatiche e tecniche di anticipazione della tutela penale. L'incriminazione dei "dual-use software"*, in *Riv. it. dir. proc. pen.*, 2017, n. 2, p. 747 ss.

SALVADORI I., *Il diritto penale dei software "a duplice uso"* in G. Fornasari e R. Wenin (a cura di), *Diritto penale e modernità: le nuove sfide fra terrorismo, sviluppo tecnologico e garanzie fondamentali. Atti del convegno Trento 2 e 3 ottobre 2015*, Napoli, 2017, p. 361 ss.

SALVI C., *Neoproprietarismo e teorie giuridiche della proprietà*, in *Europa dir. priv.*, 2020, n. 4, p. 1169 ss.

SALVINI A., voce *Estorsione e sequestro di persona a scopo di rapina o di estorsione*, in *Noviss. Dig. It.*, vol. VI, Torino, 1960, p. 1000 ss.

SAMMARCO G., *La truffa contrattuale*, Milano, 1988

SANCHIS CRESPO C. (dir.), *Fraude electrónico. Su gestión penal y civil*, Valencia, 2015

SANSOBRINO F., *Creazione di un falso account, abusivo utilizzo dell'immagine di una terza persona e delitto di sostituzione di persona*, in *Dir. pen. cont.*, 30 settembre 2014, disponibile *online* all'indirizzo http://www.penalecontemporaneo.it

SANZ MORAN A.J., *El concurso de delitos. Aspectos de política legislativa*, Valladolid, 1986

SARZANA DI S. IPPOLITO C., *Informatica e diritto penale*, Milano, 1994

SARZANA DI S. IPPOLITO C., *La legge di ratifica della Convenzione di Budapest: una "gatta" legislativa frettolosa*, in *Dir. pen. proc.*, 2008, n. 12, p. 1562 ss.

SATZGER H., *International and European Criminal Law*, München, 2018

SAXENA R., *Cyberlaundering: The Next Step for Money Launderers*, in *St. Thomas L. Rev.*, 1998, vol. 10, n. 3, p. 685 ss.

SCAPELLATO F., *Il fenomeno del riciclaggio e la normativa di contrasto*, Torino, 2013

SCHÖNKE A., SCHRÖDER H. (Hrsg.), *Strafgesetzbuch Kommentar*, München, XXX ed., 2019

SCHUMANN K.H., *Das 41. StrÄndG zur Bekämpfung der Computerkriminalität*, in *NStZ*, 2007, p. 675 ss.

SCHÜNEMANN B. *Strafrechtssystem und Betrug*, Herbolzheim, 2002

SCOPINARO L., *Internet e reati contro il patrimonio*, Torino, 2007

SCOPINARO L., *Furto di dati e frode informatica*, in *Dir. pen. proc*., 2007, n. 3, p. 364 ss.

SEIDL A., FUCKS K., *Die Strafbarkeit des Phishing nach Inkrafttreten des 41. Strafrechtsänderungsgesetzes*, in *HRRS*, 2010, n. 2, p. 85 ss.

SEMINARA S., *I soggetti attivi del reato di riciclaggio tra diritto vigente e proposte di riforma*, in *Dir. pen. proc*., 2005, n. 2, p. 233 ss.

SEMINARA S., Locus commissi delicti, *giurisdizione e competenza nel cyberspazio*, 2012, p. 7, disponibile al sito https://www.flamminiiminuto-chiocci.it/public/pubblicazioni/Giurisdizione_italiana_per_diffamazione_internet_dall_estero.pdf

SEMINARA S., *La riforma dei reati di false comunicazioni sociali*, in *Dir. pen. proc.*, 2015, n. 7, p. 813 ss.

SEMINARA S., *Spunti interpretativi sul delitto di autoriciclaggio*, in *Dir. pen. proc*., 2016, n. 12, p. 1631 ss.

SEOANE PEDREIRA A., *El delito del blanqueo de dinero: Historia, práctica jurídica y técnicas de blanqueo*, Cizur Menor, 2017

SERRANO BUTRAGUEÑO I., *Los delitos de daños*, Pamplona, 1994

SERRANO FERRER M.P., *Derecho penal y nuevas tecnologías*, Cizur Menor, 2021

SHAMSI J.A., ZEADALLY S., SHEIKH F., FLOWERS A., *Attribution in cyberspace: techniques and legal implications*, in *Security Comm. Networks*, 2016, vol. 9, n. 15, p. 2886 ss.

SICIGNANO G.J., *Money Laundering Using Cryptocurreny*, in *Athens JL*, 2021, vol. 2, n. 7, p. 253 ss.

SIEBER U., *Computerkriminalität und Strafrecht*, Köln, 1977

SIEBER U., *Computerkriminalität und Strafrecht*, Köln, 1980

SIEBER U., *The international Handbook on Computer Crime*, Chichester, 1986

SIEBER U. (eds.), *Information Technology Crime. National Legislations and International Initiatives*, in ID (eds.), *Ius Informationis. European series on Information Law*, vol. VI, Berlin, 1994

SIEBER U., *Strafrechtsvergleichung im Wandel. Aufgaben, Methoden und Theorieansätze der vergleichenden Strafrechtswissenschaft*, in U. Sieber, H. Albrecht (Hrsg.), *Strafrecht und Kriminologie unter einem Dach. Kolloquium zum 90. Geburtstag von Professor Dr. Dr. h.c. mult. Hans-Heinrich Jeschek*, Berlin, 2006, p. 78 ss.

SIEBER U., *Straftaten und Strafverfolgung im Internet*, in *NJW-Beil*., 2012, p. 86 ss.

SIEBER U., SATZGER H., VON HEINTSCHEL-HEINEGG B. (Hrsg.), *Europäisches Strafrecht*, Baden-Baden, 2014

SIMONCINI E., *Il Cyberlaundering: la «nuova frontiera» del riciclaggio*, in *Riv. trim. dir. pen. econ*., 2015, n. 4, p. 897 ss.

SIMONE A., *The strange history of ransomware: Floppy disks, AIDS research, and a Panama P.O. Box.*, in *Medium*, 2015, disponibile *online* all'idirizzo https://medium.com/un-hackable/the-bizarre-pre-internet-history-of-ransomware-bb480a652b4b.

SIXT E., *Bitcoins und andere dezentrale Transaktionssysteme. Blockchains als Basis einer Kryptoökonomie*, Wiesbaden, 2017

SGUBBI F., *Uno studio sulla tutela penale del patrimonio*, Milano, 1980

SGUBBI F., *voce Patrimonio (reati contro il)*, in *Enc. dir.*, vol. XXXII, Milano, 1982, p. 331 ss.

SGUBBI F., *Il nuovo delitto di "autoriciclaggio": una fonte inesauribile di "effetti perversi" dell'azione legislativa*, in *Dir. pen. cont*. 2015, n. 1, p. 137 ss.

SOLA L., *Tutela dei beni immateriali e reati contro il patrimonio: alcune osservazioni*, in *Ind. Pen*., 1990, n. 3, p. 782 ss.

SOTIS C., *Il ''concorso materiale apparente'': confine tra artt. 15 e 81 c.p*., in *Giur. It*., 2020, n. 1, p. 189 ss.

SPAGNUOLO M., MAGGI F., ZANERO S., *Bitiodine: Extracting intelligence from the bitcoin network* in Christin N., Safavi-Naini R. (eds.), *International Conference on Financial Cryptography and Data Security*, Berlin, 2014, pp. 457 ss.

SPIEZIA F., *International cooperation and protection of victims in cyberspace: welcoming Protocol II to the Budapest Convention on Cybercrime*, in *ERA Forum*, 2022, vol. 23, n. 1, p. 101 ss.

STESSENS G., *Money laundering*, in *Rev. Int. de Droit Penal*, 2006, vol. 77, p. 201 ss.

STURZO L., *Bitcoin e riciclaggio 2.0*, in *Dir. pen. cont.*, 2018, n. 5, p. 19 ss.

SUÁREZ GONZÁLEZ C., *Delitos contra el patrimonio y contra el orden socioeconómico*, in G. Rodriguez Mourullo (dir.), A. Jorge Barreiro (coord.), *Comentarios al código penal*, Madrid, 1997, 674 ss.

SUÁREZ GONZÁLEZ C., *Concurso de delitos: propuesta de regulación con vista a un Código penal europeo,* in K. Tiedemann, A. Nieto Martín (dir.), *Eurodelitos. El derecho penal económico en la Unión Europea,* Cuenca, 2003, p. 59 ss.

ŠEMBERA V., PAQUET-CLOUSTON M., GARCIA S., ERQUIAGA M., *Cybercrime Specialization: An Expose of a Malicious Android Obfuscation-As-A-Service*, in *2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 2021, p. 213 ss.

TADDEI ELMI G., *Corso di informatica giuridica*, Napoli, 2007

TIEDEMANN K., *Wirtschaftsstrafrecht und Wirtschaftskriminalität*, vol. II *Besonderer Teil*, Reinbek bei Hamburg, 1976

TIEDEMANN K., *Wirtschaftsstrafrecht*, München, 2017

TRABUCCHI A., *Istituzioni di Diritto Civile*, L ed. a cura di G. Trabucchi, Milano, 2022

TRAPERO BARREALES M. A., *¿Son punibles los daños informáticos imprudentes? Un debate (peligrosamente) abierto*, in *RECPC*, 2022, n. 24-18, p. 1 ss.

TROPINA T., *Organized Crime in Cyberspace*, in H. Böll-Stiftung e R. Schönenberg (eds.), *Transnational Organized Crime. Analyses of a Global Challenge to Democracy*, 2013, Bielefeld, p. 47 ss.

TROPINA T., *Fighting money laundering in the age of online banking, virtual currencies and internet gambling*, in *ERA Forum*, 2014, n. 15, p. 69 ss.

VADALÁ R.M., *Criptovalute e cyberlaundering: novità antiriciclaggio nell'attesa del recepimento della Direttiva (UE) 2018/1673 sulla lotta al riciclaggio mediante il diritto penale*, in *Sist. pen*, 6 maggio 2020

VADALÀ R.M., *La tutela penale della sicurezza degli scambi economici digitali*, 2021, disponibile al sito https://iris.univr.it

VAGENA E., NTELLIS P., *Cybersecurity Legislation: Latest Evolution in the EU and Their Implementation in the Greel Legal System*, in T. Synodinou, P. Jougleux, C. Markou, T. Prestitou (eds.), *EU Internet Law in the Digital Era*, Cham, 2020, p. 239 ss.

VALERIUS B., *Zur Strafbarkeit virtueller Sit-ins im Internet*, in E. Hilgendorf (Hrsg.), *Dimensionen des IT-Rechts*, Berlin, 2008, p. 19 ss.

VAN HARDEVELD G. J., WEBBER C., O'HARA K., *Discovering credit card fraud methods in online tutorials*, in *Proceedings of the Workshop on Online Safety, Trust and Fraud Prevention. ACM Web Science Conference*, New York, 2016, p. 1 ss.

VAN HARDEVELD G. J., WEBBER C., O'HARA K., *Deviating From the Cybercriminal Script: Exploring Tools of Anonymity (Mis)Used by Carders on Cryptomarkets*, in *Am. Behav. Sci.*, 2017, Vol. 61, n. 11, p. 1244 ss.

VAN NGUYEN T., *The modus operandi of transnational computer fraud: a crime script analysis in Vietnam*, in *Trends Organ. Crim.*, 2022, n. 25, p. 226 ss.

VAN WEGBERG R., OERLEMANS J., VAN DEVENTER O., *Bitcoin money laundering: mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin*, in *J. Financ. Crime*, 2018, vol. 25, n. 2, p. 419 ss.

VASEK M., MOORE T., *Analyzing the Bitcoin Ponzi Scheme Ecosystem*, in AA. VV., *Financial Cryptography and Data Security. FC 2018. Lecture Notes in Computer Science*, 2019, Heidelberg, p. 101 ss.

VARDI N., *Alcune considerazioni sulla natura giuridica dei Bitcoin*, in *Dir. inf. inf.*, 2015, n. 3, p. 443 ss.

VAYANSKY I., KUMAR S., *Phishing – challenges and solutions*, in *Comput. Fraud secur.*, 2018, n. 1, p. 15 ss.

VELASCO NÚÑEZ E., *Fraudes informáticos en Red: del* phishing *al* pharming, in *LL*, 2007, n. 37, p. 57 ss.

VELASCO NÚÑEZ E., *Estafa informática y banda organizada. Phishing, pharming, smishing y «muleros»*, in *La ley penal*, 2008, n. 49, p. 1 ss.

VELÁSCO NÚÑEZ E., SANCHIS CRESPO C., *Delincuencia informática. Tipos delictivos e investigación. Con jurisprudencia tras la reforma procesal y penal de 2015*, Valencia, 2019

VIGANÒ F., PIERGALLINI C. (a cura di), *Reati contro la persona e contro il patrimonio*, Torino, 2015

VON HEINTSCHEL-HEINEGG B. (Hrsg.), *Beck Online Kommentar Strafgesetzbuch*, LIII Ed., München, 2022, disponibile *online* all'indirizzo https://beck-online.beck.de

VON LISTZ F., SCHMIDT E., *Lehrbuch des deutschen Strafrechts*, Berlin, 1927

VOß M., *Die Tatobjekte der Geldwäsche*, Berlin, 2007

WACHTER M., *Grundfälle zum Computerbetrug*, in *JuS*, 2017, p. 723 ss.

WALDEN I., *Harmonising Computer Crime Laws in Europe*, in *Eur. J. Crime Crim. Law Crim. Justice*, 2004, vol. 12, n. 4, p. 321 ss.

WALTHER S., *Eigenverantwortlichkeit und strafrechtliche Zurechnung: Zur Abgrenzung der Verantwortungsbereiche von Täter und "Opfer" bei riskantem Zusammenwirken*, Freiburg im Brisgau, 1991

WANG P., SU M., WANG J., *Organized crime in cyberspace: how traditional organized criminal groups exploit the online peer-to-peer lending market in China*, in *Brit. J. Criminol.*, 2021, n. 61, p. 303 ss.

WEBER A., *Die Strafbarkeit von Plattformbetreibern im Darknet*, Baden-Baden, 2022

WEZEL H., *Das Deutsche Strafrecht. Eine systematische Darstellung*, XI ed., Berlin, 1969 (ristampa 2011)

WHITTY M.T., *Is There a Scam for Everyone? Psychologically Profiling Cyberscam Victims*, in *Eur. J. Crim. Policy Res.*, 2020, n. 26, p. 399 ss.

WILLELMS E., *Cyberdanger. Understanding and Guarding Against Cybercrime*, Cham, 2019

VIGEVANI G.E., *Anonimato, responsabilità e trasparenza nel quadro costituzionale italiano*, in *Dir. inf. inf.*, n. 2, 2014, p. 207 ss.

WÜST M., *Die Underground Economy des Darknets. Die Strafbarkeit des Betreibens „illegaler" Handelsplattformen*, Berlin, 2022

YERMACK D., *Is Bitcoin a real currency? An economic appraisal*, in *NBER Working Paper No. 19747*, 2014, p. 16 s, disponibile *online* al sito https://www.nber.org/papers/w19747

YI S., XU Z., WANG G., *Volatility connectedness in the cryptocurrency market: Is Bitcoin a dominant cryptocurrency?*, in *Int. Rev. Financ. Anal.*, 2018, vol. 60, p. 98 ss.

YOO Y.B., *Codekartenmißbrauchen am POS-Kassen-System. Strafrechtliche Überlegungen zur Computerkriminalität*, Frankfurt am Main, 1997

YU S., *Distributed Denial of Service Attack and Defense*, New York, 2014

ZACCARIA A., SCHMIDT-KESSEL M., SCHULZE R., GAMBINO A.M. (eds.), *EU eIDAS Regulation. Article-by-Article Commentary*, München, 2020

ZAGREBELSKY V., *Reato continuato*, Milano, 1976

ZANCHETTI M., *Il riciclaggio di denaro proveniente da reato*, Milano, 1997

ZANCHETTI M., voce *Ricettazione*, in *Dig. disc. pen.*, vol. XIX, Torino, 1997, p. 174 ss.

ZANNOTTI R., *La truffa*, Milano, 1993

ZHANG M., WANG L., JAJODIA S., SINGHAL A., *Network Attack Surface: Lifting the Concept of Attack Surface to the Network Level for Evaluating Networks' Resilience Against Zero-Day Attacks*, in *IEEE Trans. Dependable Secure Comput.*, 2021, vol 18, n.1, p. 310 ss.

ZHU A., FU P., ZHANG Q., CHEN Z., *Ponzi scheme diffusion in complex networks*, in *Physica A*, 2017, Vol. 479, p. 128 ss.

ZÖLLER M., *Die Strafbarkeit des Betreibens krimineller Handelsplattformen im Internet – Der neue § 127 StGB*, in *Int. Cybersecur. Law Rev.*, 2021, n. 2, p. 279 ss.

ZÖLLER M., *Strafbarkeit des Betreibens krimineller Handelsplattformen im Internet. Kritische Bemerkungen zum Regierungsentwurf vom 10.2.2021*, in *KriPoZ*, 2021, n. 2, p. 79 ss.

ZUGALDIA ESPINAR J.M., *Los delitos contra la propriedad, el patrimonio y el orden socioeconomico en el nuevo codigo penal. Consideraciones generales sobre el Título XIII del N.C.P.*, in *Cuadernos de política criminal*, 1996, n. 59, p. 417 ss.